DOI:10.20033/j.1003-7241.(2025)10-0115-05

一种基于区块链与代理重加密的医院财务数据加密算法

张 扬,钱 颖,张子伊,张丽湘
(苏州大学 附属第二医院,江苏 苏州 215004)

摘 要:针对信息共享技术中容易发生的数据安全性问题,此次研究提出一种区块链数据共享的代理重加密算法,并将其应用于医院财务管理平台中。该模型能对数据进行动态调整。研究对所提方法进行了性能测试和医院财务数据加密仿真实验。结果显示,在数据容量为 128 B 的情况下,在加密和解密的过程中分别用了 39.98 ms 和 9.77 ms;且无论数据大小为 128 B 还是 1024 B,研究方案加密和解密的运行时间均短于对照方案。由此,研究所提方法在数据加密控制领域具有较为广泛的应用前景。

关键词:区块链;代理重加密;医院财务;数据共享
中图分类号:TP309 **文献标志码**:A **文章编号**:1003-7241(2025)10-0115-05

A hospital financial data encryption algorithm based on blockchain and proxy re-encryption

ZHANG Yang, QIAN Ying, ZHANG Ziyi, ZHANG Lixiang
(The Second Affiliated Hospital of Soochow University, Suzhou 215004, China)

Abstract: Aiming at the data security problem which is easy to occur in information sharing technology, this study proposed a proxy re-encryption algorithm for controlled sharing of blockchain data, and applied it to the hospital financial management management platform. The model can dynamically adjust the data. The performance test of the proposed method and the simulation experiment of hospital financial data encryption are carried out. The results show that when the data capacity is 128 B, 39.98 ms and 9.77 ms are used in the process of encryption and decryption, respectively. No matter the data size is 128 B or 1024 B, the encryption and decryption time of the study scheme is shorter than that of the control scheme. Therefore, the proposed method has a broad application prospect in the field of data encryption control.
Keywords: blockchain; proxy reencryption; hospital finance; data sharing

0 引言

随着大数据应用的不断发展,人们对数据共享的需求也日益增加。然而,保障数据隐私在数据共享中面临着更大的挑战[1]。传统的数据中心化解决方案由于数据不可信问题,给构建有效的数据共享体系带来了极大的障碍,许多学者都对此展开了讨论[2]。黄玮为解决传统信息管理系统存在局限性、基于全息数字水印技术设计了医院财务信息管存系统,该系统可同时存储的财务数据总量大[3]。张春晖为准确划分医院财务预算数据类型,提出了一种基于主元分析方法的管理系统,以提升医院财务预算信息化管理水平[4]。唐飞等针对数据存储和安全传输问题,提出了一种基于加密的高效传输机制[5]。郭庆等提出了一种代理重加密的区块链数据共享方案,以实现权限动态调整[6]。总的来说,当前的研究主要集中在提高医院财务信息系统的稳定性和安全性,采用加密和区块链技术的策略已经得到了广泛的应用和研究。然而,现有方案虽能够在一定程度上增强数据的安全性,但是整体的操作复杂、应用效果不佳,仍然具有较大的进步空间。有鉴于此,此次研究将加密技术应用至医院信息化系统中,旨在提升医院财务管理中的数据安全性,以助力医院工作效率的提升。此次研究的创新点在于将基于区块链与代理重加密的数据加密控制系统应用于医院财务管理平台中,以提高医院财务数据的安全性和稳定性,并且构建了一种适合于有控制的区块链数据共享的代理重加密算法。

*基金项目:江苏省医院协会研究项目(JSYGY-2021-JY41)
收稿日期:2024-04-23

1 加密控制系统模型及其在医院财务管理中的应用

1.1 基于区块链与条件代理重加密的数据加密控制系统模型

区块链技术是一种新兴技术,其来源于比特币的底层抽象。在区块链中,数据信息被组织为一个个区块,并在彼此之间进行连接,形成了一个链。区块链的核心特点包括去中心化、防篡改、可追溯以及匿名性等方面[7]。区块链可根据公开程度分为以下 3 种类型:公有链、私有链和联盟链。其中,联盟链适用于多种应用场景,因此成为许多项目的底层区块链模式。

代理重加密(proxy re-encryption,PRE)是一种基于公开密钥的授权交换技术。代理重加密将加解密操作分离,以完成数据共享和解密权限的转移[8]。为了确保数据的

存储和共享安全，此次研究采用区块链技术和代理重加密技术。方案模型如图 1 所示，数据发送者使用其私钥、数据产生者的私钥和条件摘要对数据加密，生成数据密文，并将其传送至云服务器。产生数据时，数据发送者选择条件摘要，通过一系列计算生成条件摘要密文，并将其发送给区块链。当数据请求者想要获得数据时，将向联盟区块链生成搜索陷门。区块链判断是否匹配和是否交易成功。云服务器对其进行重加密，生成重加密密文。

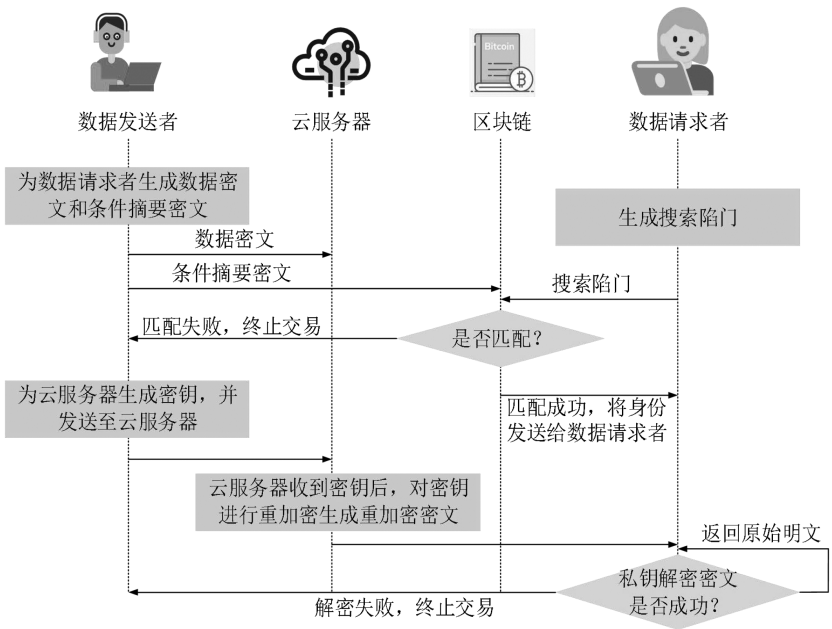


图 1　基于区块链与条件代理重加密的数据加密控制系统

此次研究方案的实施过程分为 4 个步骤，即系统搭建，交易信息上传，数据存取，用户权限更新。初始化系统参数后，系统产生公私钥对，为

$$\begin{aligned} sk_A &= x \\ pk_A &= xP \end{aligned} \tag{1}$$

式中，sk_A 表示私钥；pk_A 表示公钥；x 表示随机数；P 表示经系统初始化后的参数。在上传交易信息阶段中，数据拥有者使用初始交易密文，构造代理重加密密钥。最终代理重加密密钥的函数表达式为

$$rk_{A\to B} = H_1(rpk_A) \oplus H_1(rpk_B \parallel \alpha) \tag{2}$$

式中，rpk_A，rpk_B 表示代理重加密密钥参量；α 表示授权参数；H_1 表示系统参数。

接下来就是数据存取阶段，用户请求区块链对数据进行存取。合法用户对从区块链上获取的重加密密文的解密计算步骤为

$$\begin{aligned} M' &= C_2' \oplus H_1(sk_B C_1' \parallel \alpha) \\ k &= H_4(M' \parallel C_1' \parallel C_3') \end{aligned} \tag{3}$$

式中，M' 表示数据明文；C_1'，C_2'，C_3' 表示交易密文；sk_B 表示重加密密文。

最后一步是对用户进行身份验证的过程。在此过程中，数据持有者和区块链系统的授权管理人员会根据自己的授权清单进行交易数据的存取，从而达到对区块链数据进行动态调整的目的。

1.2　数据加密控制系统在医院财务中的应用

财务管理是医院加强管理的重要方面之一，不仅要扩大财务管理领域的参与，还要满足更广泛的财务活动内容范围[9]。区块链技术可通过存储、交换与验证节点信息，保证平台数据信息的安全与稳定[10-13]。因此，引入区块链和代理重加密的数据加密控制系统，以加强医院财务管理数据的安全性和稳定性。首先，建立医院财务私钥，其函数表达式为

$$SK_S = (K = g^{a-t_s},\ g^{a\varphi_i},\ L = g^{t_s}, K_x = H_1(x)^{t_s}) \tag{4}$$

式中，φ_i 表示域；a 表示生成元参数；K 表示用户访问文件；t_s 表示用户选取的生成元；L 表示用户获取文件；$H_1(x)$ 表示用户选取生成元后形成的文件；g 表示用户访问请求[14]。

在云环境中，对医院财务数据加密，需要将访问权限相同的数据分配至同一个集合中。假设文件的访问结构为 $(\boldsymbol{M},\rho)$，即 $\boldsymbol{M}$ 表示某一矩阵，ρ 表示函数，ρ 为 $\boldsymbol{M}$ 的映射。随机选取某一共享密钥 s 和向量 $\boldsymbol{v}$，则用户 A、B、C 的对称密钥计算公式为

$$\begin{aligned} A_1 &= KF \cdot e(g,g) \\ B_1 &= (g^a) \cdot (\rho(1)) \\ C_1 &= g^{r_j} \cdot (\rho(e)) \end{aligned} \tag{5}$$

式中，e 表示双线性映射；KF 表示随机建立的对称密钥。由此，密钥密文的函数表达式为

$$CT = (\boldsymbol{M},\rho), A_1, A_2, A_3(B_1, C_1), \cdots, (B_l, C_l) \tag{6}$$

式中，$\{\rho(i) \mid 1 \leqslant i \leqslant l\}$ 表示访问结构 $(\boldsymbol{M},\rho)$ 中的属性。将文件、密钥、密文发送给服务器进行验证，若正确，则保

留该文件、密钥、密文。随后,进行代理重加密,其计算公式为

$$C'_{(M',\rho')}=(A'=e(g,g)^{a\varphi_i},\ A_2'=g^{s'},\ B_1'=(g^{a}))\cdot H_1(\rho(1)) \tag{7}$$

式中,s' 表示重加密后的共享密钥。

加密前后的密文是一模一样的,加密过程不会对密文造成任何影响。在构建一个现代化的医院财务管理平台时,区块链技术的整合成了一个不可或缺的环节。这项技术的引入不仅提高了财务管理的效率和透明度,还显著地降低了操作成本,同时大幅度地增强了数据安全性,从而避免了潜在的数据篡改和其他安全问题[15]。要在医院财务管理平台中实施区块链技术,需进行深入的规划。这包括对平台的功能、目标用户群体、既定目标和潜在影响的周全考量[16]。此次研究以某具体医院为例,深入分析了区块链技术在其财务管理平台上的应用。研究内容涵盖了多个核心模块,如图 2 所示。这些模块包括但不限于:财务数据录入、处理和存储;交易验证和审计;资金流管理;以及合规性监控等。利用区块链的不可篡改性设计每个模块,以确保数据的真实性和完整性,同时通过智能合约自动化多个流程,从而提升运营效率。

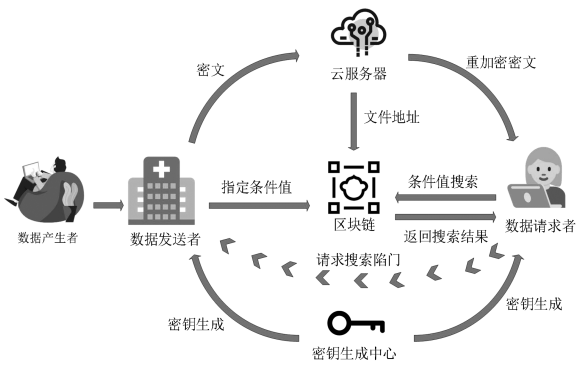


图 2 基于区块链技术的医院财务平台建设

构建基于区块链技术的医院财务平台,可以有效地实现医院财务信息的透明化、模块化和安全性,同时也可以提高医院财务管理的效率。其系统框架如下:1)数据生产者:病人到不同级别的医院就诊,获取原始数据,并将产生的医疗财政数据存入其中。每一笔交易都会形成一个块,并被加入区块链中;2)数据发送者:医院各科室均为数据发送方,中央服务器负责对医疗财务信息进行加密,并将其发送到云服务器,这一流程受各科室主管人员的控制,负责处理财务流程中的各种业务逻辑,例如资金的转移、费用的结算、报销的审批等;3)数据请求者:药品供应仓库、医院各科室等机构组成的数据需求方。资料要求方必须从资料发送者处取得搜寻陷阱,并搜寻区块链上的条件总结,并且符合某些条件的方能取得存取权;4)密钥产生中心:通过建立系统的全局结构,将公开、私有密钥分别发给请求方和发送方,从而保证了系统的安全性;5)云服务器:具备较强的运算与储存功能,主要负责对已加密的医院财务数据进行保存,并将其转化为可由使用者直接解密的密文。

2 模型性能验证及其在医院财务管理中的应用效果

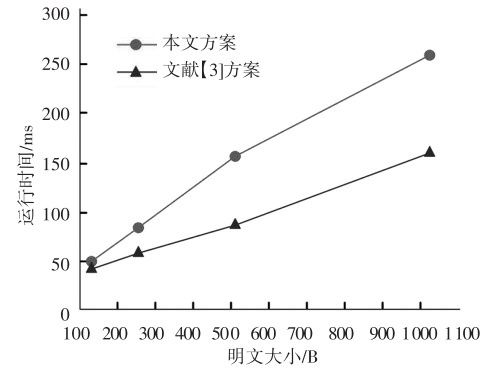
2.1 加密控制系统模型性能验证

此次研究的实验主机配备了 IntelCorei7-8700CPU,具有高达 3.20 GHz 的处理速度。内存方面,实验机配备了 8 GB 的 RAM,足够支撑 Python 脚本和所需的数据处理操作。操作系统为 Windows 10,可以提供必要的系统服务以及方便的开发环境。实验所使用的编程语言是 Python3.7.4。此次研究构建了一个包含 20 个节点的模拟网络环境,以此来评估所提数据加密控制方案的计算效率。这些节点被配置为互相交换数据,模拟真实世界中医院财务管理平台的通信场景。为了全面测试方案在处理不同大小数据时的性能,实验选取了四种典型的数据明文大小:128 B、256 B、512 B 和 1 024 B。这些大小代表了从简单的交易记录到较复杂财务报表的数据范围。每个节点分别对这四种大小的数据进行加密和解密操作,运行 100 次以确保结果的稳定性和可靠性。

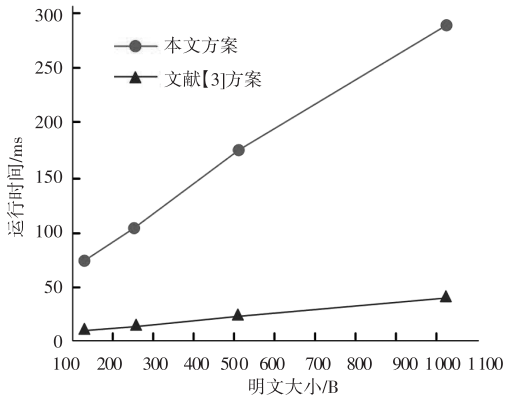
通过对算法运行 100 次取平均值进行实验结果统计,图 3 显示了加密和解密阶段的运行时间。结果显示,无论是在加密还是在解密过程中,研究方案都比文献[3]方法有效。128 B 和 1 024 B 下,所提方法在加密与解密方面的速度都更快。在数据容量为 128 B 的情况下,该方法在加密和解密过程中分别用了 39.98 ms 和 9.77 ms;文献[3]需要 49.88 ms 的密码和 71.98 ms 的解密。在 1 024 B 的情况下,所提算法分别用时为 157.78 ms 和 40.43 ms。因此,研究所提出的方法具有计算开销小的特点,并能够很好地满足区块链交易数据共享的实际需求。

本研究使用基于分布式的加密算法,并在加密过程中对加密算法的耗时性能进行了验证。试验中设定了 20 个节点和 10 个属性。从图 4 中显示的密钥数量与执行时间关系可以看出,在密钥数量为 1 的情况下,所需的处理时间是 68.98 ms。由于局部密钥数越多,产生的密钥所需要的时间越长。本项目所提算法与已有文献[3]中所提算法相比,效率更高。

图 5 为对加密、重加密和解密过程的执行时间进行了测试结果。为了更好地凸显此次研究方法的优越性,实验还选取了文献[1]中基于 Struts 框架的加密方案和文献[11]中基于联盟区块链的加密方案进行对比测试。试验证明,该方案的加密、再加密和解密所需的时间是随着使用者身份信息数目的增多而线性递增的。与文献[3]、文献[1]中的方案相比,研究方案具有更低的计算开销,证实了其优越性。



（a）加密阶段



（b）解密阶段

图 3　算法运行时间比较

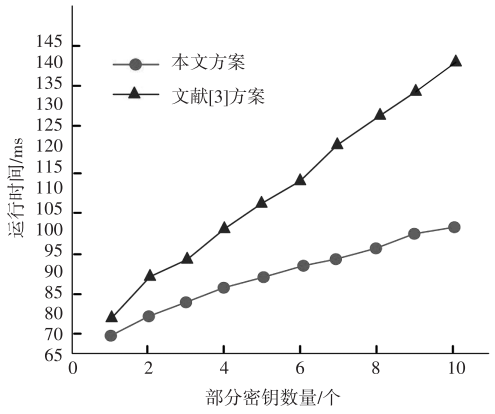
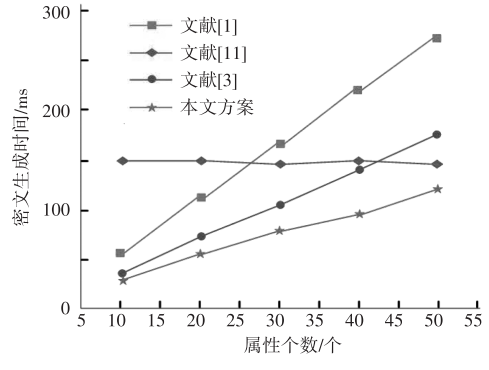
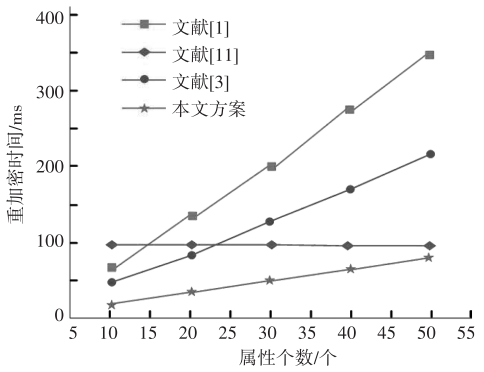


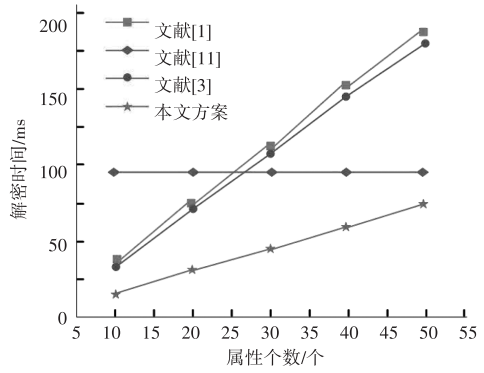
图 4　密钥生成耗时



（a）密文生成时间



（b）重加密时间



（c）解密时间

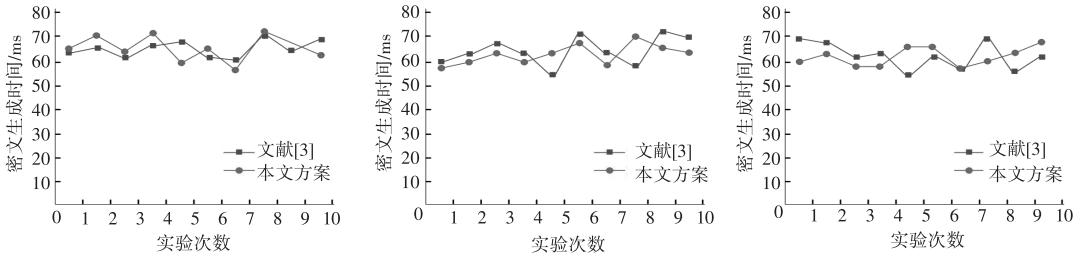
图 5　不同加密算法的耗时情况

2.2　加密控制系统医院财务仿真效果分析

医院财务管理系统截图如图 6 所示。该系统可记录门诊划价收费、收费统计、用药费用、医师收益明细及汇总、门诊费用说明等财务信息，可以确保每笔交易的透明度和不可篡改性。此外，系统中的数据加密选项是通过基于区块链与代理重加密的方案来实现的。由此，医院可以在确保数据安全性的同时，提高财务管理的效率和透明度。

图 6　医院财务管理系统截图

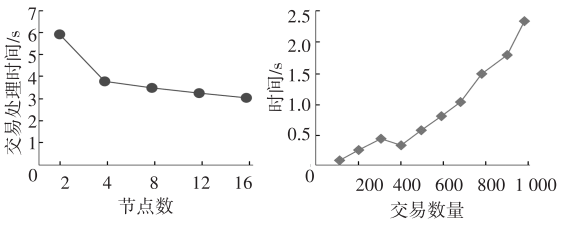
为了测试医院财务报表隐私数据加密方法的性能，此次研究进行了一系列仿真实验，并进行了应用效果分析。实验对象为 12 Gbit 规模的医院财务报表隐私数据，研究采用了 1 024 的单组序列采样长度和 120 的训练样本数进行加密。根据这些参数，实验得到了不同测试样本的加密性能输出，详见图 7。实验还将研究方法与文献[3]中的方法进行了对比，以更好地评估本方法的性能。结果表明，研究提出的医院财务报表隐私数据加密方法能够有效抵御攻击，并且加密后样本输出的置乱性更高，这极大地增强了数据加密的安全性。



（a）测试样本 1　　（b）测试样本 2　　（c）测试样本 3

图 7　加密输出性能测试结果

每个测试点取三次结果得到平均值，结果如图 8(a)所示。图 8(a)中，当节点从 2 台增加到 4 台时，处理效率有明显提升。随着节点数量增加，处理时间随之缩短，但效率提升速度减缓。图 8(b)中，系统处理的时间与交易个数成正比。当交易个数为 500 时，系统打包交易时间为 0.56 s，用户是可以接受的。



（a）交易打包处理率　　（b）租借交易处理率

图 8　医院财务交易处理结果

3　结束语

为了提升数据共享中数据信息的安全性和稳定性，提出了一种基于区块链与代理重加密的数据加密控制方案，并将其应用于医院财务管理平台。研究对所提方案进行了性能测试，结果显示：在加、解密的速度上，在数据容量为 128 B 的情况下，所提方案的加密过程只花了 39.98 ms，解密过程只花了 9.77 ms。在 1 024 B 的情况下，所提算法分别为 157.78 ms 和 40.43 ms。密钥生成耗时方面，当部分密钥数为 1 时，时间消耗为 68.98 ms。由于局部密钥数量逐渐增多，生成密钥所需要的时间也随之延长。研究方案相对于文献[3]中方案更具有高效性。医院财务数据加密的仿真实验结果显示，研究方案能够在样本数据不断增加的情况下保持较低的数据被破解量，因此能够实现数据的安全共享。此次研究存在一些局限性，首先，研究中的数据量相对较小，实际应用中数据量可能远大于 128 B 和 1 024 B，因此在更大的数据规模下，该方案的性能如何还需要进一步验证。其次，密钥生成时间随部分密钥数量的增加而增长，这可能会在处理大量密钥时造成效率问题。最后，当前研究未考虑重加密密钥的时间限制，这可能影响系统的安全性。在未来的工作中，这些问题和挑战需要被充分考虑和解决。

参考文献

[1] 邵猷海，王勇，杨云，等. 一种基于国密 SM4 算法的电力数据加密方法[J]. 微型电脑应用，2022，38(12)：98-100，110.

[2] 张国栋. 基于区块链技术的资产管理终端自动化运维系统[J]. 数字技术与应用，2023，41(1)：204-206.

[3] 黄玮. 基于全息数字水印技术的医院财务信息管存系统设计[J]. 自动化技术与应用，2022，41(9)：157-160.

[4] 张春晖. 基于主元分析方法的公立医院财务预算信息化管理系统[J]. 兵工自动化，2024，43(4)：46-49，76.

[5] 唐飞，陈云龙，冯卓. 基于区块链和代理重加密的电子处方共享方案[J]. 计算机科学，2021，48(S1)：498-503.

[6] 郭庆，田有亮，万良. 基于代理重加密的区块链数据受控共享方案[J]. 电子学报，2023，51(2)：477-488.

[7] 苏锷，吴槟，付安民，等. 基于代理重加密的云数据访问授权确定性更新方案[J]. 软件学报，2020，31(5)：1563-1572.

[8] 崔嵬，杨同军，苗凯. 基于代理重加密的财务数据安全共享技术[J]. 现代电子技术，2023，46(1)：74-78.

[9] 李静元. 基于时释性的代理重加密多用户数据共享[J]. 现代电子技术，2022，45(21)：77-82.

[10] 牛淑芬，陈俐霞，李文婷，等. 基于区块链的电子病历数据共享方案[J]. 自动化学报，2022，48(8)：2028-2038.

[11] 冯涛，焦滢，方君丽，等. 基于联盟区块链的医疗健康数据安全模型[J]. 计算机科学，2020，47(4)：305-311.

[12] 郭银章，刘尚. 基于云计算多授权中心的 CP-ABE 代理重加密方法[J]. 网络与信息安全学报，2022，8(3)：176-188.

[13] PHILIPS A，JAYARAJ J，JOSH F T，et al. Enhanced RSA key encryption application for metering data in smart grid[J]. International journal of pervasive computing and communications，2021，17(5)：596-610.

[14] 徐磊. 基于联盟区块链的医疗健康数据安全模型设计[J]. 微型电脑应用，2021，37(9)：143-154.

[15] 骆亮. 基于区块链技术的区域经济信息共享系统设计[J]. 微型电脑应用，2021，37(3)：140-143.

[16] 赵长明，薛莹，张倩. 基于区块链的链下数据保护系统优化[J]. 微型电脑应用，2022，38(1)：37-40.

作者简介：张　扬(1986—)，男，硕士，高级会计师，研究方向：财务信息化。

通信作者：张丽湘(1971—)，女，本科，高级会计师，研究方向：财务管理。