基于代理重加密的区块链数据受控共享方案

郭 庆[1,2],田有亮[1,2,3],万 良[1]
(1. 贵州大学计算机科学与技术学院,贵州贵阳 550025; 2. 贵州省公共大数据重点实验室,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)

摘 要: 区块链以分布式共享全局账本的形式存储交易数据,数据共享难以实现隐私保护和可用性之间的平衡,现有的区块链数据共享方案在进行隐私保护的同时可用性较低,有效实现区块链数据访问权限的动态调整是一个挑战性问题. 为此,本文提出基于代理重加密的区块链数据受控共享方案. 首先,基于SM2构造代理重加密算法,并借此设计区块链数据受控共享方案,利用代理重加密保护交易数据隐私实现数据安全共享. 其次,提出用户权限动态调整机制,区块链节点分工代理并对重加密密钥参数分割管理,实现用户访问权限确定性更新,交易数据的可见性得到动态调整. 最后,安全性和性能分析表明,本方案可以在保护交易隐私的同时,实现区块链数据动态共享,并且在计算开销方面具有优势,更好地适用于区块链数据受控共享.

关键词: 区块链;代理重加密;隐私保护;SM2;受控共享
基金项目: 国家自然科学基金(No.61662009,No.61772008);国家自然科学基金联合基金重点支持项目(No.U1836205);贵州省科技重大专项计划(No.20183001);贵州省科技计划项目(No.黔科合基础[2019]1098);贵州省高层次创新型人才项目(No.黔科合平台人才[2020]6008);贵阳市科技计划项目(No.筑科合[2021]1-5)
中图分类号: TP309.7 **文献标识码:** A **文章编号:** 0372-2112(2023)02-0477-12
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20210785

Blockchain Data Controlled Sharing Scheme Based on Proxy Re-Encryption

GUO Qing[1,2], TIAN You-liang[1,2,3], WAN Liang[1]
(1. *College of Computer Science and Technology*, *Guizhou University*, *Guiyang*, *Guizhou* 550025, *China*;
2. *Guizhou Provincial Key Laboratory of Public Big Data*, *Guiyang*, *Guizhou* 550025, *China*;
3. *Institute of Cryptography & Data Security*, *Guizhou University*, *Guiyang*, *Guizhou* 550025, *China*)

Abstract: The blockchain stores transaction data in the form of a distributed shared global ledger and it is difficult to achieve a balance between privacy protection and availability in data sharing. The existing blockchain data sharing schemes have low availability while protecting privacy and effectively realizing the dynamic adjustment of blockchain data access permissions is a challenging problem. To this end, this paper proposes a blockchain data controlled sharing scheme based on proxy re-encryption. Firstly, based on SM2, the proxy re-encryption algorithm is constructed to design a blockchain data controlled sharing scheme, using proxy re-encryption to protect the privacy of transaction data to achieve data secure sharing. Secondly, a dynamic adjustment mechanism of user permissions is proposed that the blockchain nodes division of labor agent and the re-encryption key parameters are dividedly managed to realize the assured update of user access rights, so that the visibility of the blockchain data can be dynamically adjusted. Finally, the security and performance analysis show that the scheme can realize the dynamic sharing of blockchain data while protecting transaction privacy, and has advantages in computing overhead, better suitable for the controlled sharing of blockchain data.

Key words: blockchain; proxy re-encryption; privacy protection; SM2; controlled sharing
Foundation Item(s): National Natural Science Foundation of China (No.61662009, No.61772008); Key Program of the National Natural Science Union Foundation of China (No.U1836205); Science and Technology Major Support Program of Guizhou Province (No.20183001); Science and Technology Program of Guizhou Province (No.[2019]1098); Project of High-level Innovative Talents of Guizhou Province (No.[2020]6008); Science and Technology Program of Guiyang (No.[2021]1-5)

收稿日期:2021-06-24;修回日期:2022-01-13;责任编辑:孙瑶

1 引言

在分布式环境下实现数据安全共享一直是研究热点. 自2008年,化名为“中本聪”的作者发表了一篇《比特币:一种点对点的电子现金系统》[1]以来,区块链作为比特币的底层技术得到了广泛的应用. 区块链是由多方共同维护的分布式账本技术,具有去中心化、可追溯、不可篡改的特点. 区块链技术的应用不仅仅局限于加密货币,还为数据安全共享提供了平台支撑. 然而,由于区块链上的交易信息对网络中全部节点公开透明,每个节点都可以读取交易数据,攻击者通过对区块链账本中数据进行分析,对用户的交易隐私和身份隐私构成威胁[2]. Noether等人[3]曾提出了基于环签名的数字货币门罗币,采用环签名来隐藏交易金额,但是该签名技术在签名过程中需要其他用户一起完成签名,交易信息易泄露,曾被追踪用户签名私钥的方式攻破了隐藏的交易. 区块链上用户身份信息和交易数据的隐私保护越来越受到研究学者的重视,交易数据安全共享面临巨大挑战.

对用户身份信息和交易数据的隐私保护是区块链技术在安全方面的关键问题. Miers等人[4]基于比特币提出可匿名的区块链数字货币方案——零币,通过零知识证明和RSA累加器等密码学技术来隐藏交易者地址、中断交易之间的关联,使得交易不可追踪,不透漏交易的相关信息,对区块链提供较高的隐私保护,但该算法证明过程非常缓慢,实用性不强. Kosba等人[5]首次在区块链中提供事务隐私和可编程性的方法,基于智能合约和零币的思想,用户向智能合约发送加密信息,虽然智能合约的结果可公开验证,但在合约中的所有交易行为的顺序要对公众保密. Maesa等人[6]实现了一种基于比特币平台的访问控制系统,该系统可以管理访问策略并通过交易实现用户之间权限的转移,访问控制策略和权限转换在区块链上是公开可见的. 随后,Maesa等人[7]又使用智能合约对该方案进行了改进,利用智能合约实现访问控制. Wang等人[8]通过同态加密技术和区块链智能合约对用户进行隐私保护,但只有交易双方对交易信息是可见的,不利于用户高效共享数据. Li等人[9]提出了一种使用区块链和无证书加密技术的分布式数据存储方案,利用区块链矿工消除了传统的集中式服务器,矿工通过无证书密码学技术来记录审计. Dong等人[10]提出了一种去中心化数据共享模型,改进交易记录格式和共识机制,借助安全多方计算和差分隐私技术保证数据隐私. Wu等人[11]提出一种基于区块链的电子病历安全共享模型,该模型使用数据脱敏技术,以牺牲某些数据准确性为代价解决了交易隐私泄露问题. 以上方案主要通过数字签名、零知识证明、同态加密等密码学技术保护身份隐私和交易隐私,区块链数据共享性局限于预先设定的数据用户,难以实现高效扩展,可用性较低,无法满足数据共享的实际需要.

针对如何实现交易数据安全共享问题,Wang等人[12]提出了一种基于区块链的数据共享与追溯方案,该方案为实现数据安全共享和数据来源的可追溯性,采用了双链结构,一条链存储原始数据,另一条链用来存储交易数据. Wu等人[13]提出了一种基于可追踪属性的加密方案,利用区块链技术保证数据的完整性和不可否认性,并且通过预加密技术快速生成密文,使用属性布隆过滤器将隐藏策略发送到区块链. Tian等人[14]提出了基于属性加密的区块链数据溯源算法,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,在保护交易隐私的同时,实现溯源信息动态共享,但是当区块上属性更新时,会增加数据追溯的复杂性. Feng等人[15]将分层属性加密与线性秘密共享相结合,提出了基于可搜索属性加密的区块链数据隐私访问控制方案,用户的访问控制由验证节点实现,避免了向区块链网络提交私钥和访问结构的风险. Wang等人[16]提出了应用区块链的数据访问控制与共享模型,利用属性基加密对企业数据进行访问控制与共享,实现数据细粒度访问控制和安全共享. 在上述方案中,当区块链交易数据访问权限变更时,需要对数据进行重复加密,加重了用户的计算量,也增加了通信开销,区块链数据高效安全共享成为亟待解决的问题.

代理重加密技术允许半可信代理者将一个用户能解密的密文转换成另一个用户能解密的具有相同明文的密文,在授权变更时无需重复加密数据,用户只需计算重加密密钥即可完成数据共享,在区块链环境中具有应用价值. 目前,代理重加密技术在数据共享中具有广泛应用. Su等人[17]提出基于代理重加密的云数据访问授权确定性更新方案,将重加密密钥进行分割管理,实现授权变更时密钥的确定性更新. 随后,Su等人[18]又针对物联网云节点提出了基于代理重加密的可信授权方案,在授权服务器的控制下确保数据共享的安全可靠. Wang等人[19]基于身份代理重加密技术,实现安全社交云数据受控共享. Deng等人[20]为实现高效数据共享,提出了一种基于混合属性的代理重加密方案,让代理服务器将属性加密的密文转换为基于身份加密的密文,使资源受限的用户可以有效地访问之前属性加密的数据. Samanthula等人[21]提出一种云计算联合的安全数据共享和查询框架,使用同态加密和代理重加密技术可防止被撤销的用户重新加入系统时泄露未经授权的数据,在该方案中是假设2个服务器不发生共谋来实现数据安全共享. 以上方案主要是利用代理重加密技术在云环境或大数据平台中实现数据共享,不适

用于在区块链上进行高效稳定的用户隐私数据共享.

鉴于上述分析,本文提出一种基于代理重加密的区块链数据受控共享方案. 利用SM2构造代理重加密算法完成交易数据隐私保护,通过对代理重加密密钥参数的管理实现数据访问权限确定性更新. 本文的主要贡献有如下几点.

(1)构造适用于区块链数据受控共享的代理重加密算法. 基于SM2加密算法设计代理重加密算法,在保护交易隐私的同时,实现区块链数据受控共享,在交易数据共享的隐私保护和可用性之间取得平衡.

(2)提出交易数据共享的用户权限动态调整机制. 区块链矿工节点分工代理并对代理重加密密钥参数分割管理,由授权管理节点验证用户数据访问权限,实现用户访问权限的确定性更新,让交易数据的可见性得到动态调整,并且授权变更时无需重复加密数据.

(3)安全性分析和性能分析表明,本文提出的方案不仅能够在保护交易隐私的同时实现数据动态共享,而且在功能性及计算开销方面更好地适应区块链网络开放环境下的数据受控共享.

2　准备知识

2.1　区块链

区块链是一种在对等网络环境下,基于透明可信共识机制,并按照时间顺序将数据区块以链条的方式组合形成的特定数据结构,并以密码学方式保证其数据不可篡改、不可伪造、可追溯的去中心化、去信任的分布式共享总账系统. 在一定时间段内的交易通过验证后,组成区块并加盖时间戳链接到区块链数据库中,随着区块的不断增多,形成一条由创始区块到最新区块的数据存储结构,可以按时间对数据进行追溯.

区块链可分为公有链、联盟链、私有链[22]. 其中,公有链是完全去中心化、非许可的区块链,任何组织或个人都可以加入,比特币和以太坊属于公有链;联盟链是部分去中心化的许可链,通常由多个机构共同参与,节点的加入需要其他联盟成员的同意,本文提出的区块链数据受控共享方案适用于联盟链;私有链通常用于单位或组织的内部系统,其数据的读写权限由该组织进行控制.

2.2　代理重加密技术

代理重加密(Proxy Re-Encryption, PRE)在公钥加密的基础上支持解密权限的转移,在1998年的欧洲密码学年会上,由Blaze等人[23]首次提出. PRE体制允许一个半可信的代理者(proxy)将Alice可解密的密文转换为Bob可解密的同一明文的密文,并且半可信代理者无法获取数据明文的任何信息. 代理重加密把加解密工作在数据共享时进行拆分,在此过程中,用户完成首次加密,代理者基于首次密文针对不同共享用户进行重加密,数据拥有者共享数据无需重复加密操作,把加密的工作交给代理服务器,减轻了工作量. 根据密文的转换方向,可将代理重加密分为单向代理重加密和双向代理重加密. 单向代理重加密只能实现Alice到Bob的密文转换,而双向代理重加密不仅能实现Alice到Bob的密文转换,还可以实现Bob到Alice的密文转换,本文构造的是单向代理重加密方案. 近年来,有学者提出了基于关键词搜索的PRE方案[24]、基于身份的PRE方案[25],把身份、属性和用于细粒度管理的密钥类型等作为PRE密钥的重要参数[17],可为密文访问控制的研究提供重要基础.

2.3　SM2加密算法

国密算法SM2的可证安全性已经达到了密码算法的最高安全级别,其实现效率相当或略高于国际标准的密码算法,相较于比特币、超级账本等现有区块链架构选用的国际通用密码算法ECC,拥有安全、稳定、高效等优势. 国密SM2加密算法由以下几个算法组成.

(1)初始化. 给定安全参数κ,生成椭圆曲线参数$\text{params}=\{p,q,E,G\}$,其中$p$是大素数,表示有限域的规模,$E$表示定义在有限域$F_p$上的椭圆曲线,$G$表示椭圆曲线$E$上阶为$q$的生成元点.

(2)密钥产生. 输入系统公开参数params,用户随机选取$d\in[1,q-1]$,计算$P=dG$,d作为私钥保存,P作为公钥公开.

(3)加密算法. 给定参数params,消息的比特串M,长度为klen,用公钥P按照如下步骤加密:

(a)用随机数发生器产生随机数$k\in[1,q-1]$;

(b)计算椭圆曲线点$C_1=[k]G=(x_1,y_1)$,将C_1的数据类型转换为比特串;

(c)计算$[k]P=(x_2,y_2)$;

(d)计算$t=\text{KDF}(x_2\|y_2,\text{klen})$;

(e)计算$C_2=M\oplus t$;

(f)计算$C_3=\text{Hash}(x_2\|M\|y_2)$;

(g)返回密文$C=(C_1,C_2,C_3)$.

(4)解密算法. 给定参数params,密文$C=(C_1,C_2,C_3)$,用私钥d解密:

(a)计算$[d]C_1=(x_2,y_2)$;

(b)计算$t=\text{KDF}(x_2\|y_2,\text{klen})$;

(c)计算$M=C_2\oplus t$;

(d)计算$C_3'=\text{Hash}(x_2\|M\|y_2)$,若$C_3'=C_3$,输出$M$.

3 系统设计

3.1 系统模型

基于代理重加密的区块链数据受控共享方案包括4类参与实体,分别是数据拥有者、数据使用者、授权管理者、维护区块链的矿工节点. 系统模型如图1所示,所包含实体及其功能说明如下.

(1)数据拥有者. 对共享交易数据加密产生初始密文,规定数据的访问权限,决定用户权限的撤销和重加入,构造代理重加密密钥,把附加了初始密文和代理重加密密钥的交易广播到区块链网络. 数据拥有者可以是矿工,也可以是区块链上进行交易的用户.

(2)数据使用者. 在区块链上请求访问交易数据,可用其私钥和解密参数对重加密密文进行解密获取共享数据.

(3)授权管理者. 区块链系统中指定的授权管理者,为了实现整个系统的去中心化,可以通过区块链共识机制选出的授权管理节点,完成节点的注册、密钥的分发,管理数据访问权限. 根据数据拥有者给定的授权列表验证用户的访问权限,把验证结果发送给其余矿工. 给合法数据用户发送解密参数,与数据拥有者交互,通过授权列表的管理实现区块链数据访问权限的更新.

(4)维护区块链的矿工节点. 对于合法用户,通过数据拥有者上传的代理重加密密钥对初始交易密文进行重加密,把交易数据的重加密密文发送给数据使用者,对于非法用户,则拒绝用户请求. 把一段时间内的数据交易记录广播,其他节点对区块进行验证后加入区块链账本.

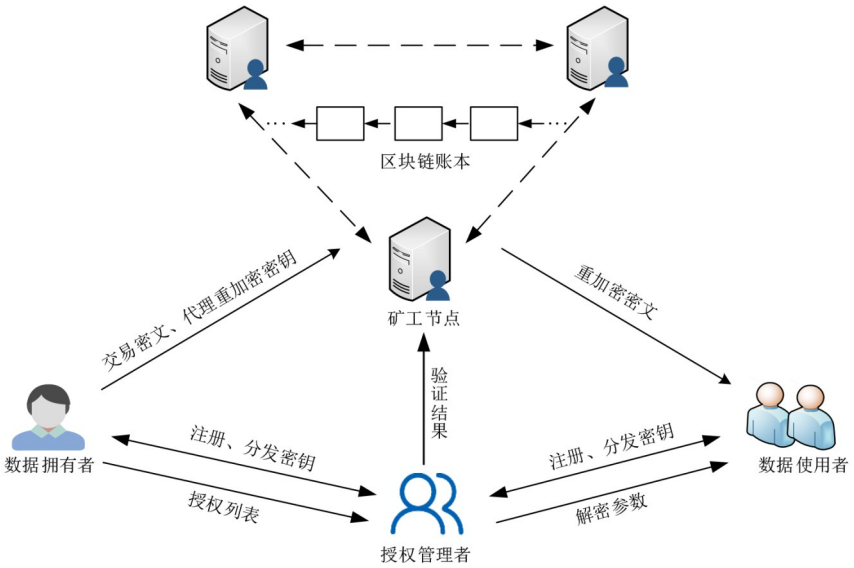


图1 系统模型

其中,授权管理者为可信实体,在本方案中存在矿工节点的潜在攻击,维护区块链系统中的矿工是“诚实且好奇”的. 由于区块链激励机制,区块链上想要获得奖励的节点会完成代理重加密操作,同时也可能会在区块链网络中获取交易密文和代理重加密密钥后进行密码分析和共谋攻击,导致用户的隐私数据泄露.

3.2 安全模型

本方案的代理重加密算法安全模型如下所述.

攻击者$\mathcal{A}$可以询问密钥生成、代理重加密密钥生成、重加密、解密等过程.

初始化:挑战者$\mathcal{C}$选择参数,生成系统初始系数pp.

阶段1:攻击者$\mathcal{A}$询问KeyGen, ReKeyPara, ReKeyGen, ReEncrypt, Decrypt任意过程. 其中,询问ReKeyPara, ReKeyGen, ReEncrypt, Decrypt时使用的密钥由KeyGen产生.

挑战:攻击者$\mathcal{A}$完成阶段1询问后,输出等长明文$(m_0, m_1) \in M$,解密参数α^*,由ReKeyPara生成的重加密参数β^*及被攻击目标的公钥pk^*,此处的pk^*由KeyGen产生,私钥未被泄露. 当攻击者$\mathcal{A}$以$(\beta^*, \beta', \alpha^*)$询问ReKeyGen函数时,$\beta'$对应的私钥是保密的. 挑战者$\mathcal{C}$选取$b \in \{0,1\}$作为随机比特,计算用于挑战询问的密文$C_b = \mathrm{Encrypt}(m_b, \mathrm{pk}^*)$.

阶段2:攻击者$\mathcal{A}$继续阶段一中的询问,同时满足以下条件.

(1)当攻击者$\mathcal{A}$以$(\beta^*, \beta', \alpha^*)$对ReKeyGen进行询问时,$\beta'$的私钥保密;

(2)当$\mathcal{A}$以$(C_b, \beta^*, \beta', \alpha^*)$对ReEncrypt进行询问时,$\mathrm{pk}'$的私钥保密;

(3)当$\mathcal{A}$以$(\beta^*,\beta',\alpha^*)$对ReKeyGen进行询问时,则不可以使用$C_b'$询问Decrypt,其中,$C_b'$是ReEncrypt$(C_b,\beta^*,\beta',\alpha^*)$的有效输出.

猜测:攻击者$\mathcal{A}$猜测$b'\in\{0,1\}$,若$b'=b$,则说明挑战成功.

若攻击者$\mathcal{A}$赢得上述挑战的优势定义为ε,则$\varepsilon=\left|\Pr[b'=b]-1/2\right|$,如果此处的$\varepsilon$可以忽略不计,则称攻击者$\mathcal{A}$挑战失败,对应的被挑战方案是选择密文安全的(CCA).

4　区块链数据受控共享方案

4.1　方案概述

首先给出本文方案的总体流程图,如图2所示.

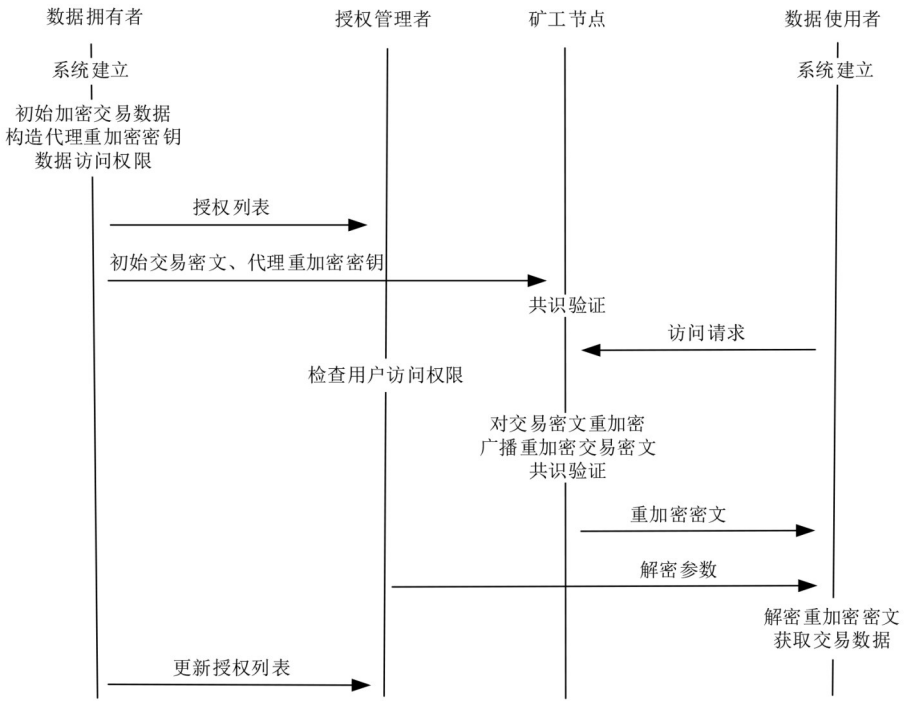


图2　方案流程图

本文方案包含系统建立、上传交易信息、数据访问、用户授权更新4个阶段.

(1)系统建立阶段. 初始化系统参数,产生公私钥对.

(2)上传交易信息阶段. 数据拥有者使用自身公钥加密交易数据产生初始交易密文,构造代理重加密密钥,划分交易数据访问权限,并把初始交易密文、代理重加密密钥广播到区块链网络,同时把授权列表发送给区块链系统的授权管理者.

(3)数据访问阶段. 用户向区块链发送数据访问请求,授权管理节点验证用户访问权限. 若为合法用户,区块链矿工节点使用数据拥有者上传的代理重加密密钥对初始交易密文进行重加密,并把重加密交易密文发送给数据使用者,同时区块链授权管理节点把解密参数发送给数据使用者,数据使用者可以用其私钥和解密参数解密重加密交易密文,获取交易数据明文. 若为非法用户,则拒绝用户请求.

(4)用户授权更新阶段. 数据拥有者与区块链系统授权管理者交互,通过更新授权列表来完成交易数据访问权限的更新,实现数据用户的撤销或者是重加入,让区块链数据的可见性得到动态调整.

4.2　方案构造

阶段1:系统建立

包含系统初始化和密钥生成2个步骤.

(1)系统初始化:Setup$(\kappa)\to$pp

给定安全参数κ,得到κbit的素数p,q,E,G. p表示有限域的规模,E表示定义在有限域F_p上的椭圆曲线,定义P为椭圆曲线E上的一点,并将其作为群G的生成元,G为q阶循环群. 定义哈希函数组H_1,H_2,H_3,H_4,其中$H_1:\{0,1\}^*\to\{0,1\}^l$,$H_2:G\to Z_q^*$,$H_3:\{0,1\}^*\to G$,$H_4:\{0,1\}^*\to G$. 公布系统参数pp=$\{p,q,E,G,P,H_1,H_2,H_3,H_4\}$.

(2)密钥生成:KeyGen$(\text{pp})\to(\text{sk}_A,\text{pk}_A)$

输入系统公开参数pp,选择随机数$x\in Z_q^*$,私钥$\text{sk}_\text{A}=x$,公钥$\text{pk}_\text{A}=xP$.

阶段2:上传交易信息

包含交易信息初始加密、生成代理重加密密钥参量、构造代理重加密密钥和授权列表.

数据拥有者使用自身公钥加密交易数据,产生初始密文,构造代理重加密密钥$\mathrm{rk}_{\mathrm{A}\to\mathrm{B}}$和授权列表$L$. 并把交易密文、代理重加密密钥$\mathrm{rk}_{\mathrm{A}\to\mathrm{B}}$广播到区块链网络,区块链上矿工节点对交易进行验证. 把授权列表L发送给区块链系统授权管理者,通过对L的管理实现区块链数据访问权限的更新. 数据拥有者对交易数据记录初始加密和生成代理重加密密钥计算如下.

(1)初始加密:$\mathrm{Encrypt}\left(M,\mathrm{pk}_{\mathrm{A}}\right)\to C$. 数据拥有者使用自身公钥$\mathrm{pk}_{\mathrm{A}}$加密消息$M$,$M$的长度为$l$,选取$i\in G$,加密运算如下:

$$r=H_2(i) \tag{1}$$

$$C_1=rP=\left(x_0,y_0\right) \tag{2}$$

$$\mathrm{rpk}_{\mathrm{A}}=\left(x_{\mathrm{A}},y_{\mathrm{A}}\right) \tag{3}$$

$$t=H_1\left(x_{\mathrm{A}}\|y_{\mathrm{A}}\right) \tag{4}$$

$$C_2=M\oplus t \tag{5}$$

$$C_3=H_3\left(x_{\mathrm{A}}\|M\|y_{\mathrm{A}}\right) \tag{6}$$

$$C_4=H_4\left(M\|C_1\|C_3\right) \tag{7}$$

$$C=\left(C_1,C_2,C_3,C_4\right) \tag{8}$$

对交易数据初始加密后上传到区块链上进行广播,矿工对交易进行验证. 数据拥有者可访问其上传的交易数据,用自身私钥解密交易密文,解密运算如下:

$$S=\mathrm{sk}_{\mathrm{A}}C_1=\left(x_{\mathrm{A}}\|y_{\mathrm{A}}\right) \tag{9}$$

$$t=H_1\left(x_{\mathrm{A}}\|y_{\mathrm{A}}\right) \tag{10}$$

$$M=C_2\oplus t \tag{11}$$

$$C_3'=H_3\left(x_{\mathrm{A}}\|M\|y_{\mathrm{A}}\right) \tag{12}$$

若$C_3'=C_3$,得到数据明文M.

(2)代理重加密密钥参量生成:$\mathrm{RekeyPara}\left(r,\mathrm{pk}_{\mathrm{A}},\mathrm{pk}_{\mathrm{B}}\right)\to\beta$. 数据拥有者构造针对数据用户B的代理重加密密钥参量,即$\beta=\left\{\mathrm{rpk}_{\mathrm{A}},\mathrm{rpk}_{\mathrm{B}}\right\}$.

(3)代理重加密密钥生成:$\mathrm{RekeyGen}\left(\alpha,\beta\right)\to\mathrm{rk}_{\mathrm{A}\to\mathrm{B}}$. 数据拥有者通过代理重加密密钥参量$\beta$以及自身定义的授权参数$\alpha$,计算出针对数据用户B的代理重加密密钥$\mathrm{rk}_{\mathrm{A}\to\mathrm{B}}$上传到区块链网络,即

$$\mathrm{rk}_{\mathrm{A}\to\mathrm{B}}=H_1\left(\mathrm{rpk}_{\mathrm{A}}\right)\oplus H_1\left(\mathrm{rpk}_{\mathrm{B}}\|\alpha\right) \tag{13}$$

阶段3:数据访问

数据用户向区块链发送数据请求,授权管理节点根据数据拥有者上传的授权列表L检查请求用户是否有访问权限,若为非法用户,则拒绝用户请求. 若为合法用户,其余矿工节点对初始交易密文进行重加密后,把重加密密文发送给请求用户.

(1)代理重加密:$\mathrm{ReEncrypt}\left(C,\mathrm{rk}_{\mathrm{A}\to\mathrm{B}}\right)\to C'$. 对于合法用户,区块链系统上矿工节点对交易密文$C$的代理重加密计算如下:

$$C_1'=C_1 \tag{14}$$

$$C_2'=\mathrm{rk}_{\mathrm{A}\to\mathrm{B}}\oplus C_2 \tag{15}$$

$$C_3'=C_3 \tag{16}$$

$$C_4'=C_4 \tag{17}$$

$$C'=\left(C_1',C_2',C_3',C_4'\right) \tag{18}$$

(2)解密:$\mathrm{Decrypt}\left(\mathrm{sk}_{\mathrm{B}},C',\alpha\right)\to M$. 合法用户从区块链上获取重加密密文后,可用其私钥和区块链授权管理者发送的解密参数α进行解密获取交易数据,用户解密重加密密文计算如下:

$$M'=C_2'\oplus H_1\left(\mathrm{sk}_{\mathrm{B}}C_1'\|\alpha\right) \tag{19}$$

$$k=H_4\left(M'\|C_1'\|C_3'\right) \tag{20}$$

若$k=C_4'$,则$M=M'$,合法用户得到交易数据明文.

阶段4:用户授权更新

区块链上的授权管理者存储授权列表L,根据数据拥有者的要求来更新数据访问权限. 区块链上的矿工节点存储原始交易密文和代理重加密密钥,根据授权管理节点的验证结果决定是否对交易密文进行重加密共享给数据用户. 数据拥有者与区块链授权管理者交互通过删除授权列表L来撤消数据请求者对数据记录的访问权限,通过更新授权列表L来授予数据请求者新的访问权限.

为了进一步具体描述区块链交易数据共享的隐私保护需求,本文抽象一个区块链系统数据共享平台,如图3所示;初始化4个参与方A,B,C,D. 定义交易数据的隐私保护需求,如表1所示. 考虑到交易数据的可见性应该根据数据拥有者的具体业务需求而定,则交易数据可由数据拥有者自身定义为基础数据和敏感数据,交易数据只有交易发起方和授权使用方可见,未授权的参与方只能看到交易数据密文. 例如,参与方A发起的交易中的基础数据,有自身和授权用户B和D可见,只有参与方C不可见. 参与方A发起的交易中的敏感数据,只有参与方A和授权用户B可见,参与方C和D都不能访问,只能看见密文和哈希值. 数据拥有者与区块链系统授权管理者交互,更新授权列表L,让交易数据的可见性得到动态调整,具体步骤如下.

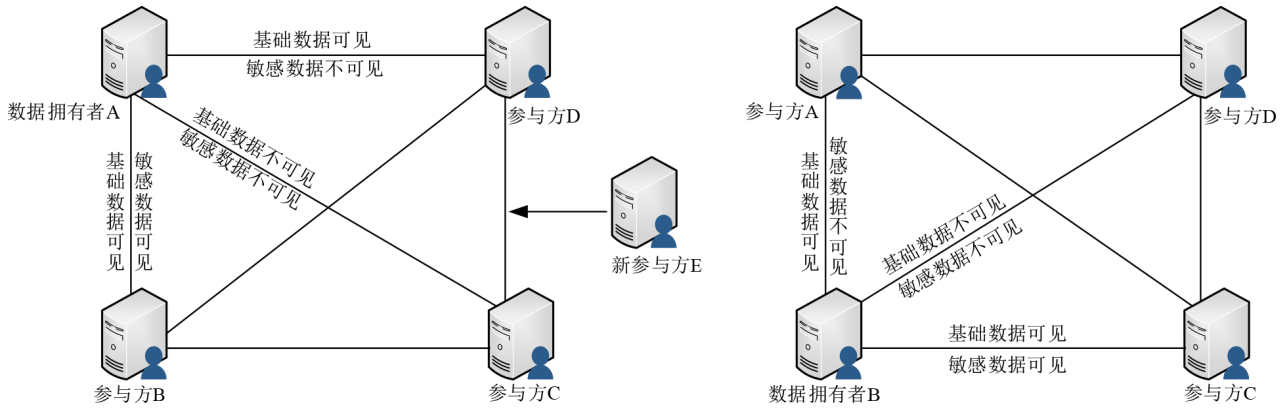
(1)数据拥有者A要授权共享交易数据中的敏感数据给原本没有访问权限的参与方D,则数据拥有者A与区块链系统授权管理者交互,更新授权列表L,添加针对数据使用者D的授权参数,同时构造对应的代理重加密密钥$\mathrm{rk}_{\mathrm{A}\to\mathrm{D}}$广播到区块链网络.

(2)数据拥有者A要授权共享交易数据给新的参与方E,则数据拥有者A与区块链系统授权管理者交互,更新授权列表L,添加针对数据使用者E的授权参

数,同时构造对应的代理重加密密钥$\mathrm{rk}_{\mathrm{A}\to\mathrm{E}}$广播到区块链网络.

(3)数据拥有者B要撤销原来合法数据用户C的访问权限,则B与授权管理者交互,删除对应的授权列表参数.

在以上授权更新过程中,数据拥有者在对交易数据进行初始加密后,后续更新访问权限不用再对数据进行重复加密,只需定义新的授权列表发送给授权管理者,以及构造对应的代理重加密密钥广播到区块链网络.



(a)　参与方A共享数据　　(b)　参与方B共享数据

图3　区块链数据共享平台

表1　交易数据隐私保护需求表

数据拥有者	交易数据类型	数据使用者			
		参与方A	参与方B	参与方C	参与方D
参与方A	基础数据	可见	可见	不可见	可见
	敏感数据	可见	可见	不可见	不可见
参与方B	基础数据	可见	可见	可见	不可见
	敏感数据	不可见	可见	可见	不可见

5　方案分析

5.1　正确性分析

初始密文$C_1=rG=(x_0,y_0)$,$C_3=H_3(x_{\mathrm{A}}\|M\|y_{\mathrm{A}})$,$C_4=H_4(M\|C_1\|C_3)$,在进行重加密计算后,$C_1'=C_1$,$C_3'=C_3$,$C_4'=C_4$. 解密时得到$M'$,$k=H_4(M'\|C_1'\|C_3')$,故只要验证$k=C_4'$,则有$M=M'$. 因此可以通过验证$k$与$C_4'$是否相等来判断解密结果是否正确.

下面分析在计算过程正确的情况下,有$M=M'$.

$$\begin{aligned}M'&=C_2'\oplus H_1(\mathrm{sk}_{\mathrm{B}}C_1'\|\alpha)\\&=\mathrm{rk}_{\mathrm{A}\to\mathrm{B}}\oplus C_2\oplus H_1(\mathrm{sk}_{\mathrm{B}}C_1'\|\alpha)\\&=H_1(\mathrm{rpk}_{\mathrm{A}})\oplus H_1(\mathrm{rpk}_{\mathrm{B}}\|\alpha)\oplus C_2\\&\quad\oplus H_1(\mathrm{sk}_{\mathrm{B}}C_1'\|\alpha)\end{aligned}\tag{21}$$

其中,$\mathrm{sk}_{\mathrm{B}}C_1'=\mathrm{sk}_{\mathrm{B}}C_1=\mathrm{sk}_{\mathrm{B}}(rP)=r(\mathrm{sk}_{\mathrm{B}}P)=\mathrm{rpk}_{\mathrm{B}}$,则$H_1(\mathrm{sk}_{\mathrm{B}}C_1'\|\alpha)=H_1(\mathrm{rpk}_{\mathrm{B}}\|\alpha)$,则有

$$\begin{aligned}M'&=H_1(\mathrm{rpk}_{\mathrm{A}})\oplus C_2\\&=H_1(\mathrm{rpk}_{\mathrm{A}})\oplus M\oplus H_1(\mathrm{rpk}_{\mathrm{A}})\\&=M\end{aligned}\tag{22}$$

所以在计算过程正确的情况下,有$M=M'$,因此本文方案是正确的.

5.2　安全性分析

定义1　DDH复杂性假设:对于任意$a,b\in Z_q^*$,给定一个循环群G上的一组元素$P,aP,bP,T\in G$,判断等式$T=abP$是否成立是困难的.

定理1　若DDH复杂性假设在群G上成立,则本文的代理重加密方案在随机预言机模型下是CCA安全的.

证明　算法中有4个哈希计算,下面分析过程将其模拟成四个不同的随机谕示,这4个计算中的哈希计算过程输入取值空间不同,可以自动区分为不同的哈希操作. 算法中的4次哈希操作可采用安全的哈希算法SM3代替随机谕示. 证明定理1即证明攻击者$\mathcal{A}$以优势ε进行挑战,则$\varepsilon=\left|\Pr[b'=b]-1/2\right|$可以忽略. 定义挑战游戏$\mathcal{G}_i(i=0,1,2,\cdots,5)$,挑战者$\mathcal{C}$定义$T_i$表示在$\mathcal{G}_i$中$b'=b$的事件.

(1)$\mathcal{G}_0$:挑战者$\mathcal{C}$如实回答攻击者$\mathcal{A}$的随机询问,同时初始化$H_i^{\mathrm{list}}(i=1,2,3,4)$,令$\delta_0=\Pr[b'=b]$,则$\left|\delta_0-1/2\right|=\varepsilon$.

(2)$\mathcal{G}_1$:挑战者$\mathcal{C}$同$\mathcal{G}_0$进行该游戏,除了如下内容. 挑战者$\mathcal{C}$随机选择$\tau\in\{1,2,\cdots,p+1\}$,对$H_1$进行$\tau$次询问,当$\mathcal{C}$接到攻击者$\mathcal{A}$的挑战后,若攻击者$\mathcal{A}$为对$H_1$进

行问询则挑战者终止游戏，挑战者$\mathcal{C}$成功的概率至少为$1/(p+1)$，$\mathcal{G}_1$中$\delta_1=\Pr[b'=b]$，则$\Pr[T_1]=\delta_1/(p+1)$.

(3)$\mathcal{G}_2$：挑战者$\mathcal{C}$同$\mathcal{G}_1$进行游戏，除了H_i发生碰撞，由于哈希函数为标准的随机过程，因此$\left|\Pr[T_1]-\Pr[T_2]\right|$可忽略.

(4)$\mathcal{G}_3$：挑战者$\mathcal{C}$同$\mathcal{G}_2$进行游戏，仅在调用Decrypt时有区别，若输入为(C,β^*,α^*)，攻击者$\mathcal{A}$没有对H_1使用$(\beta^*\|\alpha^*)$询问，挑战者则终止游戏，否则挑战者$\mathcal{C}$返回解密结果给攻击者$\mathcal{A}$. 由于加解密算法过程确定，且所使用的哈希函数为随机过程，因此$\left|\Pr[T_2]-\Pr[T_3]\right|$可忽略.

(5)$\mathcal{G}_4$：挑战者$\mathcal{C}$同$\mathcal{G}_3$进行游戏，除了在调用ReKeyGen，ReEncrypt时有区别.

调用ReKeyGen中，挑战者$\mathcal{C}$使用攻击者$\mathcal{A}$提出的(β,α)对重加密密钥列表进行查询，若有结果在，挑战者$\mathcal{C}$为攻击者$\mathcal{A}$反馈$\mathrm{rk}_{\mathrm{A}\to\mathrm{B}}$，若没有结果，挑战者$\mathcal{C}$在密钥列表中，依据$\beta,\alpha$查询，计算$\mathrm{rk}_{\mathrm{A}\to\mathrm{B}}=H_1(\mathrm{rpk}_{\mathrm{A}})\oplus H_1(\mathrm{rpk}_{\mathrm{B}}\|\alpha)$. 若用户的私钥泄露，则挑战者反馈终止. 在调用ReEncrypt中，挑战者$\mathcal{C}$使用攻击者$\mathcal{A}$提出的(β,α,C_i)计算ReEncrypt中的解密参数，若不成立，则挑战者$\mathcal{C}$反馈终止，否则在密钥和重加密密钥列表中进行密钥查询，为攻击者$\mathcal{A}$反馈密文. 若攻击者$\mathcal{A}$在ReKeyGen中使用的pk_i不是通过KeyGen获取的，则挑战者终止游戏.$\left|\Pr[T_3]-\Pr[T_4]\right|$可忽略.

(6)$\mathcal{G}_5$：挑战者$\mathcal{C}$同$\mathcal{G}_4$进行游戏，除了在接到攻击者$\mathcal{A}$的挑战(m_0,m_1,α)后，挑战者$\mathcal{C}$计算首次解密的密文，选取$i\in G$，计算$r=H_2(i)$，$C=(C_1,C_2,C_3,C_4)$，$C_1=rP=(x_0,y_0)$，$\mathrm{rpk}_{\mathrm{A}}=(x_{\mathrm{A}},y_{\mathrm{A}})$，$t=H_1(x_{\mathrm{A}}\|y_{\mathrm{A}})$，$C_2=M\oplus t$，$C_3=H_3(x_{\mathrm{A}}\|M\|y_{\mathrm{A}})$，$C_4=H_4(M\|C_1\|C_3)$. 则$\mathcal{G}_5$和$\mathcal{G}_4$的区别在于是否对$H_2$进行查询，对$H_2$进行问询的难度基于DDH问题，因此$\left|\Pr[T_4]-\Pr[T_5]\right|$可忽略. 由于Hash函数是随机过程，因此$\Pr[T_5]=1/2(p+1)$.

基于以上分析，

$$\left|\Pr[T_1]-\Pr[T_5]\right|=\left|\frac{\delta_0}{p+1}-\frac{1}{2(p+1)}\right|=\left|\frac{\delta_0-1/2}{p+1}\right|=\frac{\varepsilon}{p+1}$$

可忽略，即ε是可以忽略的. 证毕

定理2 若本文的代理重加密算法满足CCA安全，则本文区块链数据受控共享方案具有隐私保护性.

证明 首先，区块链系统中任何有效的操作都会以交易的形式记录在区块上，交易双方都通过在区块链上的地址共享数据，区块链账户具有匿名性，攻击者即使获取了交易记录tx，也无法通过交易密文提取到用户的真实身份，因此本方案可以保护用户身份隐私. 其次，交易数据经过初始加密后上传到区块链上，由于区块链激励机制，想要获取奖励的矿工节点会对初始交易密文进行代理重加密后共享给合法数据用户，根据本文的代理重加密算法满足CCA可知，即便攻击者获取到交易密文，也无法从中获取到有关明文的任何有效信息，因此本方案可以保护交易隐私. 综上，本文区块链数据受控共享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3 若本文的授权管理节点是可信的，则区块链数据具有动态共享性.

证明 交易信息tx上链前由数据拥有者A用其公钥进行初始加密，并且划分了数据的访问权限，构造针对合法用户B的代理重加密密钥$\mathrm{rk}_{\mathrm{A}\to\mathrm{B}}$，把授权列表$L$发送给了区块链授权管理者，满足访问权限的数据用户可以从交易密文C'中共享到交易信息. 本方案在区块链上可通过共识机制选出可信的授权管理节点，实现数据访问权限的确定性更新. 当交易信息的访问权限发生变化时，授权管理者更新授权列表为L'，区块链上矿工节点根据授权管理者验证结果产生新的代理重加密密文. 故旧数据用户无法通过其私钥和α获取到有效交易信息，而新的数据用户可以用其私钥和解密参数α'对新的重加密交易密文进行有效访问. 故区块链数据具有动态共享性. 证毕

定理4 若本文代理重加密算法满足CCA安全，则本文方案可以抵抗共谋攻击.

证明 在本方案中，任意用户之间的共谋只会获取他们所授权访问的数据，授权用户B与代理方共谋也只能获取用户B被授权访问的数据，下面主要指非法用户或者被撤销用户与代理方之间的共谋. 首先，区块链上的矿工节点对初始交易密文进行代理重加密操作，攻击者需要与区块链系统上超过半数的节点共谋，即51%攻击，显然代价极大. 其次，即使攻击者成功和区块链系统上矿工节点共谋，获取了初始交易密文$C=(C_1,C_2,C_3,C_4)$和代理重加密密钥$\mathrm{rk}_{\mathrm{A}\to\mathrm{B}}=H_1(\mathrm{rpk}_{\mathrm{A}})\oplus H_1(\mathrm{rpk}_{\mathrm{B}}\|\alpha)$，掌握了交易密文转换的主动性，可计算出重加密密文$C'=(C_1',C_2',C_3',C_4')$，$C_1'=C_1$，$C_2'=\mathrm{rk}_{\mathrm{A}\to\mathrm{B}}\oplus C_2$，$C_3'=C_3$，$C_4'=C_4$，但交易数据始终以密态的形式在区块链网络中传输.

根据本文代理重加密算法满足CCA安全可知，交易数据明文不会被泄露. 本文结合代理重加密技术和区块链技术，构造分布式数据共享方案，把密文转化的任务委托给一个去中心化的区块链系统来完成，具有抗共谋攻击的性质，可实现密态数据信息安全共享. 证毕

6　性能分析

6.1　方案对比

Noether等人[3]提出了基于环签名的保密交易方案,通过环签名的方式隐藏交易金额、保护交易隐私和身份隐私.Tian等人[14]基于属性加密提出区块链数据溯源算法,设计适用于区块链的策略更新算法,实现了交易隐私的动态保护.Feng等人[15]将分层属性加密与线性秘密共享相结合,提出了一种基于可搜索属性加密的区块链数据隐私保护控制方案,对没有访问权限的节点隐藏交易信息,有权限的区块链节点可通过陷门关键字查询到交易的有效信息,解决了传统区块链交易中的隐私暴露问题.Zyskind等人[26]提出了一种区块链保护隐私数据的模型,使用区块链智能合约判断用户的访问权限,利用对称或非对称的方式加密存储数据,只能进行一对一的数据安全传输.Wang等人[12]提出了一种基于区块链技术的数据共享方案,介绍了一种区块链双链结构,结合代理重加密技术,实现了安全可靠的数据共享.本文方案结合SM2加密算法和代理重加密技术,对重加密密钥的产生参数分割管理,在重加密密钥的确定性更新下,对区块链数据访问权限动态更新,实现了区块链数据的受控共享.下面针对是否支持密文数据访问控制、是否可以抵抗共谋攻击、权限的更新是否具有确定性、是否重加密,以及区块链的数据溯源性等方面,把本方案与现有研究方案进行功能特性对比分析,如表2所示.

表2　本文方案与现有研究方案对比

方案	密文访问控制	抗共谋攻击	授权确定性更新	重加密	可追溯
文献[3]	×	√	×	×	√
文献[14]	√	×	√	×	√
文献[15]	√	√	×	×	√
文献[26]	√	×	×	×	×
文献[12]	√	×	×	√	√
本文	√	√	√	√	√

6.2　计算效率分析

为了说明本方案的运算效率,本文列举了现有研究方案进行对比,定义符号T_E表示指数运算,T_P表示双线性配对运算,T_H表示哈希运算,T_M表示群中元素点乘运算,XOR表示异或运算.在表3中,给出了本方案与文献[18]等方案的性能计算对比分析.

表3　方案性能计算对比

方案	初始加密	重加密	解密
文献[18]	$3T_E+T_P+4T_H$	$2T_E+2T_P+3T_H$	$3T_E+2T_P+3T_H$
文献[27]	$3T_E+2T_P+T_H$	T_E+T_P	$T_E+T_P+T_H$
文献[12]	$2T_E+T_P+3T_H$	T_P+4T_H	T_E+T_P
文献[28]	$4T_M+2T_H+$XOR	XOR	$5T_M+2T_H+$XOR
本文	$2T_M+4T_H+$XOR	XOR	T_M+2T_H+XOR

在上述方案的运算中,双线性配对运算和指数运算会消耗较多的计算资源,Su等人[18]的方案用云服务器存储数据并进行代理重加密,完成物联网云节点间的数据共享,计算量较大.Kim等人[27]的方案同样用代理服务器完成代理重加密过程,实现轻量级设备如传感器的数据共享.Wang等人[12]的方案数据源提供商把重加密密钥上传到区块链上,数据请求者从区块链上获取重加密密钥后完成密文转换的任务,再用其私钥进行解密,增加了用户的计算量.Chen等人[28]的方案使用区块链智能合约来完成代理重加密,计算量较小,实现了去中心化的数据共享,但没有进行数据访问权限的动态更新.本方案基于SM2构造轻量级的代理重加密算法,计算开销较小,可以满足区块链交易数据共享实际需要,同时可实现区块链数据访问权限的动态调整.

6.3　实验分析

本文的实验主机配置为3.20 GHz,i7-8700 CPU,8 GB RAM,系统为Windows10,编程语言为Python 3.7.4.采用SM2椭圆曲线公钥密码算法标准中推荐的素数域256位椭圆曲线,即$y^2=x^3+ax+b$,曲线参数如表4所示.

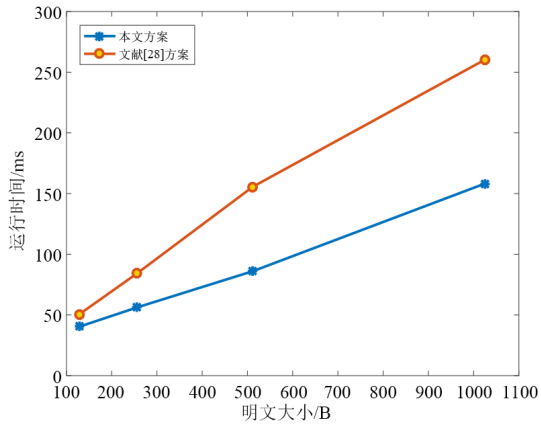
表4　SM2公钥密码算法椭圆曲线参数

曲线参数	取值
p	FFFFFFFEFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF00000000FFFFFFFFFFFFFFFF
a	FFFFFFFEFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF00000000FFFFFFFFFFFFFFFC
b	28E9FA9E9D9F5E344D5A9E4BCF6509A7F39789F515AB8F92DDBCBD414D940E93
n	FFFFFFFEFFFFFFFFFFFFFFFFFFFFFFFF7203DF6B21C6052B53BBF40939D54123
x_G	32C4AE2C1F1981195F9904466A39C9948FE30BBFF2660BE1715A4589334C74C7
y_G	BC3736A2F4F6779C59BDCEE36B692153D0A9877CC62A474002DF32E52139F0A0

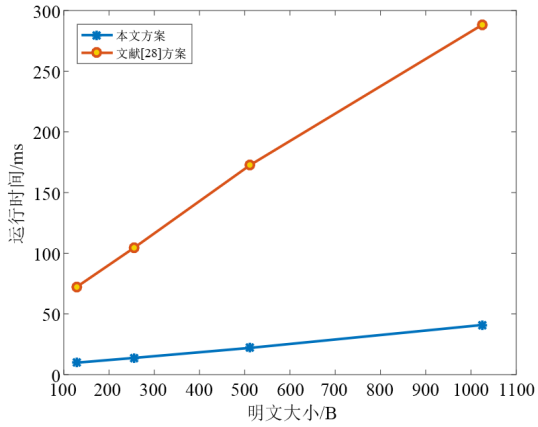
将本文方案与文献[28]方案的运行效率进行分析比较,通过改变数据明文的大小来分析本文方案的计算效率,明文大小分别取128 B,256 B,512 B,1 024 B,实验结果取算法运行100次的平均值,如图4所示.加

密阶段包括初始加密和代理重加密部分，解密阶段表示对重加密密文的解密.

从图4可知，本文方案在加密阶段和解密阶段的运行效率均高于文献[28]方案. 例如在数据大小为128 B时，本文方案加密阶段运行时间为40.25 ms，解密阶段运行时间为9.82 ms，文献[28]方案加密所需时间为50.43 ms，解密所需时间为72.08 ms. 当数据大小为1 024 B时，本文方案加密耗时158.09 ms，解密耗时40.88 ms，计算开销较小，可以满足区块链交易数据共享的实际需要.



(a) 加密阶段



(b) 解密阶段

图4 算法运行时间比较

为完整模拟整个交易信息的上链、数据访问，本文实验利用4台主机采用Python编写PBFT共识算法对区块链数据共享操作进行模拟. 共识节点用SQL Server 2008存储本地区块数据，以提高区块存储和数据访问效率. 交易信息上链过程分为对交易数据初始加密、构造代理重加密密钥、共识验证、写入本地区块4个步骤，数据访问过程分为权限验证、代理重加密、共识验证、对重加密交易密文解密4个步骤. 从图5中可以看出，当数据大小在1 024 B以内时，上述过程操作的执行时间维持在700 ms以内，并且时间代价随数据大小的增加呈线性增长趋势.

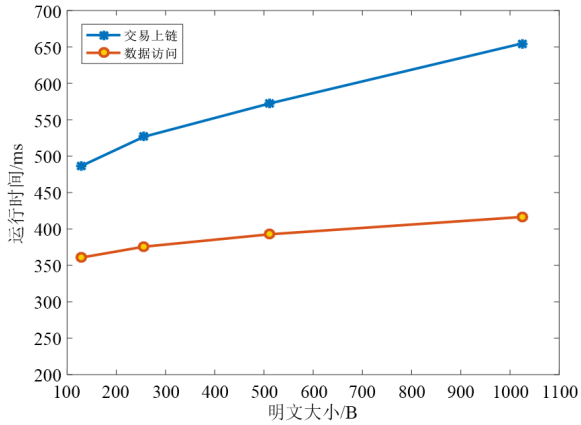


图5 数据共享执行时间代价

7 结论

针对区块链数据共享的隐私安全问题，本文提出一种基于代理重加密的区块链数据受控共享方案. 数据上链过程中，基于SM2构造适用于区块链数据受控共享的代理重加密算法，实现交易数据共享的隐私保护. 交易信息访问过程中，通过对代理重加密密钥参数分割管理完成数据访问权限的更新，让交易数据的可见性得到动态调整. 安全性和性能分析表明，本方案可以在保护用户隐私的同时实现交易数据动态共享，计算效率和现有的研究方案相比也有一定的提升，在安全性、功能性和计算开销方面整体具有较大优势，在区块链数据共享的隐私保护和可用性之间取得有效平衡. 本方案符合联盟链部分去中心化和保护交易数据隐私的要求，可适用于利用区块链分布式数据库来共享敏感数据的应用场景，如个人隐私数据、法律文件、电子病历等，因此如何在具体应用场景中结合区块链技术设计高效合理的数据共享方案将是下一步的研究工作.

参考文献

[1] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system[EB/OL]. [2021-3-26]. http://bitcoin.org/bitcoin.pdf.

[2] 祝烈煌, 高峰, 沈蒙, 等. 区块链隐私保护研究综述[J]. 计算机研究与发展, 2017, 54(10): 2170-2186.
ZHU L H, GAO F, SHEN M, et al. Survey on privacy preserving techniques for blockchain technology[J]. Journal of Computer Research and Development, 2017, 54(10): 2170-2186. (in Chinese)

[3] NOETHER S, MACKENZIE A, RESEARCH LAB T M. Ring confidential transactions[J]. Ledger, 2016, 1: 1-18.

[4] MIERS I, GARMAN C, GREEN M, et al. Zerocoin: Anon-

ymous distributed E-cash from bitcoin[C]//2013 IEEE Symposium on Security and Privacy. Berkeley: IEEE, 2013: 397-411.

[5] KOSBA A, MILLER A, SHI E, et al. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts[C]//2016 IEEE Symposium on Security and Privacy. San Jose: IEEE, 2016: 839-858.

[6] DI FRANCESCO MAESA D, MORI P, RICCI L. Blockchain based access control[C]//IFIP International Conference on Distributed Applications and Interoperable Systems. Cham: Springer, 2017: 206-220.

[7] DI FRANCESCO MAESA D, MORI P, RICCI L. Blockchain based access control services[C]//2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data. Halifax: IEEE, 2018: 1379-1386.

[8] WANG R, TSAI W T, HE J, et al. A medical data sharing platform based on permissioned blockchains[C]//ICBTA 2018: Proceedings of the 2018 International Conference on Blockchain Technology and Application. Xi'an: ACM, 2018: 12-16.

[9] LI R N, SONG T Y, MEI B, et al. Blockchain for large-scale Internet of Things data storage and protection[J]. IEEE Transactions on Services Computing, 2019, 12(5): 762-771.

[10] 董祥千, 郭兵, 沈艳, 等. 一种高效安全的去中心化数据共享模型[J]. 计算机学报, 2018, 41(5): 1021-1036.
DONG X Q, GUO B, SHEN Y, et al. An efficient and secure decentralizing data sharing model[J]. Chinese Journal of Computers, 2018, 41(5): 1021-1036. (in Chinese)

[11] WU S H, DU J. Electronic medical record security sharing model based on blockchain[C]//Proceedings of the 3rd International Conference on Cryptography, Security and Privacy. Melmaruvathur: ACM, 2019: 13-17.

[12] WANG Z, TIAN Y L, ZHU J M. Data sharing and tracing scheme based on blockchain[C]//2018 8th International Conference on Logistics, Informatics and Service Sciences (LISS). Toronto: IEEE, 2018: 1-6.

[13] WU A X, ZHANG Y H, ZHENG X K, et al. Efficient and privacy-preserving traceable attribute-based encryption in blockchain[J]. Annals of Telecommunications, 2019, 74 (7/8): 401-411.

[14] 田有亮, 杨科迪, 王缵, 等. 基于属性加密的区块链数据溯源算法[J]. 通信学报, 2019, 40(11): 101-111.
TIAN Y L, YANG K D, WANG Z, et al. Algorithm of blockchain data provenance based on ABE[J]. Journal on Communications, 2019, 40(11): 101-111. (in Chinese)

[15] FENG T, PEI H M, MA R, et al. Blockchain data privacy access control based on searchable attribute encryption [J]. Computers, Materials & Continua, 2020, 66(1): 871-890.

[16] 王秀利, 江晓舟, 李洋. 应用区块链的数据访问控制与共享模型[J]. 软件学报, 2019, 30(6): 1661-1669.
WANG X L, JIANG X Z, LI Y. Model for data access control and sharing based on blockchain[J]. Journal of Software, 2019, 30(6): 1661-1669. (in Chinese)

[17] 苏铓, 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.
SU M, WU B, FU A M, et al. Assured update scheme of authorization for cloud data access based on proxy re-encryption[J]. Journal of Software, 2020, 31(5): 1563-1572. (in Chinese)

[18] SU M, ZHOU B, FU A M, et al. PRTA: A proxy re-encryption based trusted authorization scheme for nodes on CloudIoT[J]. Information Sciences, 2020, 527: 533-547.

[19] WANG X A, XHAFA F, MA J F, et al. Controlled secure social cloud data sharing based on a novel identity based proxy re-encryption plus scheme[J]. Journal of Parallel and Distributed Computing, 2019, 130: 153-165.

[20] DENG H, QIN Z, WU Q H, et al. Flexible attribute-based proxy re-encryption for efficient data sharing[J]. Information Sciences, 2020, 511: 94-113.

[21] SAMANTHULA B K, ELMEHDWI Y, HOWSER G, et al. A secure data sharing and query processing framework *via* federation of cloud computing[J]. Information Systems, 2015, 48: 196-212.

[22] 马晓婷, 马文平, 刘小雪. 基于区块链技术的跨域认证方案[J]. 电子学报, 2018, 46(11): 2571-2579.
MA X T, MA W P, LIU X X. A cross domain authentication scheme based on blockchain technology[J]. Acta Electronica Sinica, 2018, 46(11): 2571-2579. (in Chinese)

[23] BLAZE M, BLEUMER G, STRAUSS M. Divertible protocols and atomic proxy cryptography[M]//Lecture Notes in Computer Science. Berlin: Springer, 1998: 127-144.

[24] SHAO J, CAO Z F, LIANG X H, et al. Proxy re-encryption with keyword search[J]. Information Sciences, 2010, 180(13): 2576-2587.

[25] WANG H B, CAO Z F, WANG L C. Multi-use and unidirectional identity-based proxy re-encryption schemes[J]. Information Sciences, 2010, 180(20): 4042-4059.

[26] ZYSKIND G, NATHAN O, PENTLAND A S. Decentralizing privacy: Using blockchain to protect personal data [C]//2015 IEEE Security and Privacy Workshops. San Jose: IEEE, 2015: 180-184.
[27] KIM S, LEE I. IoT device security based on proxy re-encryption[J]. Journal of Ambient Intelligence and Humanized Computing, 2018, 9(4): 1267-1273.
[28] CHEN B W, HE D B, KUMAR N, et al. A blockchain-based proxy re-encryption with equality test for vehicular communication systems[J]. IEEE Transactions on Network Science and Engineering, 2021, 8(3): 2048-2059.

作者简介

郭 庆 女,1997年出生,贵州铜仁人. 硕士研究生. 主要研究方向为密码学与区块链技术.
E-mail: qingguo_gq@163.com

田有亮(通讯作者) 男,1982年出生,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、区块链与电子货币. 中国电子学会会员编号:E190029411M.
E-mail: youliangtian@163.com

万 良 男,1974年出生,贵州铜仁人. 博士,贵州大学教授,硕士生导师. 主要研究方向为网络空间安全.
E-mail: wanliangtr@163.com