基于区块链的可代理健康档案访问方案

王 迪 刘芳芳 久美草 芦殿军*
(青海师范大学数学与统计学院 青海 西宁 810008)

摘 要 将区块链作为数据存储平台的个人健康档案安全访问方案是当下研究的热点。区块链上数据不可篡改的特点,有效保证了数据的安全。因此基于区块链的特性,提出一种基于区块链的个人健康档案安全访问方案,在该方案中,患者提前将其个人健康档案的访问权限授予代理签名者,授权信息存储在代理签名者所属的授权机构私有链中,确保在患者不可控的情况下,医生仍可以对其个人健康档案进行正常访问。该方案满足不可抵赖性和不可伪造性,且具有较高的安全性和较低的运算量。

关键词 区块链 个人健康档案 数字签名 访问方案

中图分类号 TP3 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2024.07.045

THE SECURE ACCESS SCHEME OF PERSONAL HEALTH FILES BASED ON BLOCKCHAIN

Wang Di Liu Fangfang Jiu Meicao Lu Dianjun*
(*School of Mathematics and Statistics, Qinghai Normal University, Xining 810008, Qinghai, China*)

Abstract The security access scheme of personal health files using blockchain as a data storage platform is a hot research topic. The data on the blockchain cannot be tampered with, effectively ensuring the security of the data. Therefore, based on the characteristics of blockchain, a secure access scheme for personal health files based on blockchain is proposed. In this scheme, the patient granted the proxy signer the access rights to his personal health file in advance, and the authorization information was stored in the private chain of the authorized institution to which the proxy signer belonged, so as to ensure that doctors could still have normal access to their personal health files under the circumstances beyond the control of patients. The scheme satisfied non-repudiation and unforgeability, and had higher security and lower computational complexity.

Keywords Blockchain Personal health record Digital signature Access plan

0 引 言

随着区块链技术开始应用于社会各个领域,其对数据的安全隐私保护功能,逐渐被医学领域的学者关注。2016 年 Liu[1] 从病历、区块链和大数据三个方面对在医疗记录存储和检索上使用区块链的优缺点进行了讨论,同时对病历的完整性、查看控制权限等特点进行了分析和总结。Yue 等[2] 基于区块链提出了一种构建医疗保健数据网关的方法,患者在确保隐私不被泄露的情况下,实现数据的安全控制和共享,同时该方法实现了第三方在不受信任却不侵犯患者隐私的前提下对数据进行计算。2018 年 Hölbl 等[3] 基于区块链对以患者为中心的医疗保健系统进行了分析,综述了系统的潜在应用,强调了在医疗保健领域中应用区块链技术的挑战。2019 年,Beinke 等[4] 在确定了电子健康记录的主要利益相关群体及其需求后,提出了一种基于区块链的电子健康记录架构,同时讨论了利用区块链技术在提高电子健康档案方面的潜力。Alex 等[5] 针对分布在不同医疗服务提供商之间医疗数据统一视图难以获得的问题,提出了一种基于区块链技术的分布式电子健康记录模型,该模型通过对来自不同数据库的病历进行分析,证明了其具有较低的平均响应时间和较高的可用性。2020 年,Agbo 等[6] 介绍了区块链技

收稿日期:2021 - 01 - 09。青海省应用基础研究计划项目(2019-ZJ-7099)。**王迪**,硕士生,主研领域:代数组合与密码学。**刘芳芳**,硕士生。**久美草**,硕士生。**芦殿军**,教授。

术在医疗保健领域中的应用,并分析了其中存在的安全隐私、利益相关者的参与问题。Tanwar 等[7]探讨了利用区块链技术改善医疗保健系统局限性的几种方案,并提出一种基于超电子医疗保健记录访问的共享系统,该系统可改善医疗保健提供者之间数据的可访问性,提高了效率和安全性。

同样,互联网信息技术的发展使得个人医疗档案也逐步趋于电子化,如何保证电子档案的安全性,已成为研究的热门问题。2016 年,Chen 等[8]利用公钥加密体制和拉格朗日插值多项式的方法,构造了一种具有高安全性、高效率的加密方案,该方案保证了用户的电子健康记录能够被安全访问。2017 年,Pussewalage 等[9]提出一种具有受控访问委托功能的访问控制方案,该方案在用户行为不适当的情况下,限制了允许授权的总数,同时加入了撤销机制,防止属性串谋攻击。Marwan 等[10]于 2018 年针对云计算中存在的安全和隐私问题,提出了一种医疗机构之间的多方安全计算协议,该协议利用同态加密的方法,确保了医疗数据的隐私性。2019 年,Tang 等[11]针对医疗行业中数据的访问控制和隐私泄露等问题,提出了一种有效保护隐私的云雾辅助健康数据共享方案,该方案通过对患者和雾节点的访问策略相结合的方法,增强了健康数据的安全性和抗合谋能力。Edemacu 等[12]于 2020 年提出了一种高效、抗合谋的即时用户撤销的访问控制方案,该方案实现了电子健康数据的安全共享,并利用有序二元决策图的访问结构,实现了前向安全性和后向安全性。

区块链在对数据的安全保密性上存在着巨大的优势,而保证个人健康档案数据的安全,正是建立个人健康档案的首要前提。因此,区块链技术与个人健康档案的安全访问相结合在医疗领域中是一个重大的突破。2016 年 Azaria 等[13]提出了一个基于区块链的处理分散电子病历记录的管理系统,该系统利用区块链实现了信息保密、数据共享及隐私安全,解决了供应商的数据存储问题,促进了供应商间的相互操作。2017 年 Dubovitskaya 等[14]针对医疗服务提供商之间的电子健康记录数据共享问题,提出了基于区块链的医疗数据管理和共享框架,该框架保证了数据的隐私性和安全性。Xia 等[15]针对保护云之外的医疗数据传播、隐私泄露等问题,利用区块链的不变性和内置自治性,提出了一个基于区块链的数据共享框架,该框架允许被邀请且通过验证的用户访问,保证了方案的可靠性,同时该方案具有可扩展性和高效性。Dagher 等[16]于 2018 年提出了一个基于区块链的可增强访问控制和数据混淆的智能合约框架,该框架保护了患者敏感信息的隐私,同时保证了患者、提供者和第三方之间数据的安全性、相互操作性和高效性。Thwin 等[17]针对区块链中有限存储、隐私泄露、许可撤销等问题,利用代理重加密技术提出了一种基于区块链的秘密数据共享模型。Nagasubramanian 等[18]提出了一种基于区块链的云中无密钥签名的电子健康记录系统,该系统利用云计算进行身份验证,并提供完整的运行状况记录,减少了存储空间和应用成本。2020 年,Arunkumar 等[19]设计了一个安全、分散且基于云的医疗区块链,该区块链利用加密算法、智能代码等方法,解决了患者医疗数据在与不同医疗机构交换时的隐私安全问题。

上述研究工作主要基于云中或者在区块链网络中,针对电子病历的数据共享和隐私安全等问题的解决方法,少量文献提及了患者如何保证对自己健康档案访问的知情权和控制权。同时不同机构间病历的互操作困难,跨机构间的病历传输一直是一个难点。少部分利用区块链中的智能合约或者工作量证明等方法,但并未详细说明。

因此,本文利用区块链的私有链构建患者的健康档案,设计一种基于区块链的个人健康档案访问方案。该方案针对患者在不可控的情况下,利用代理授权方法,将患者的访问权限授予给代理签名者,保证医生仍可以对其个人健康档案进行正常访问,并加入聚合签名保证患者在就诊的过程中,医生的诊断结果及患者的各项检查结果都真实可追溯。同时在数据的传输以及加密过程中,设计详细的加密方法,确保了隐私安全。虽然并未全部解决区块链医疗领域内所面临的困难问题,但是有一定程度上的进步。

1 数据结构与系统模型

1.1 数据结构

区块链中的数据区块简单来说是由多个交易信息和部分区块信息组成的数据账本。私有链中区块数据结构大体相同,如图 1 所示。

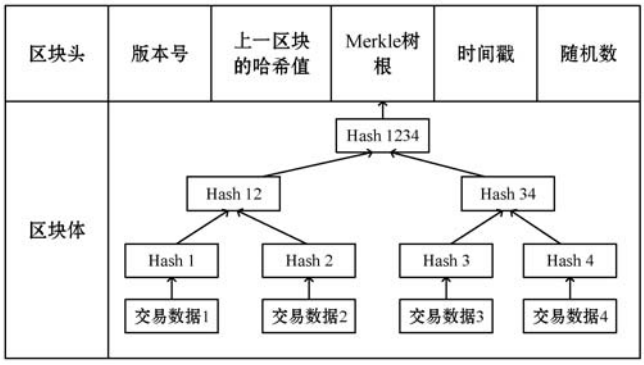

图 1 区块的数据结构

块的数据结构如图 1 所示,它由区块头和区块体构成。区块头包括版本号、上一个区块的哈希值、Merkle 树根、时间戳、随机数。区块体中是区块的交易信息,它包括交易数量字节数、交易数量和交易数据。在家庭私有链、授权机构私有链、医疗机构私有链中,链中的区块数据结构相同,其不同之处在于所在区块体中存储的交易数据之间的差别。

假设每个家庭构建家庭私有链,患者属于家庭中的一员,每一位家庭成员为家庭私有链中的一个节点;授权机构拥有属于本机构的私有链,代理签名者属于机构中的一员,每一位代理签名者为授权机构私有链中的一个节点,授权机构私有链中包含验证节点;医疗机构拥有属于该机构的私有链,医疗机构中包括主治医生和检查医生,每一位医生为医疗机构私有链一个节点,医疗机构私有链中包含验证节点。

授权机构私有链:授权机构私有链上的交易数据由产生者身份 I_{D_B}、授权证书 w_{BP}、代理签名私钥 x'_p 和产生者代理签名者的签名构成。同一代理签名者,会在一定的时间范围内代理多名患者,代理成功后,会生成与其代理对应的交易数据。生成的交易数据,将会以一定时间长度为单位生成区块,多个区块构成授权机构私有链。

医疗机构私有链:医疗机构中的私有链由签名的患者个人健康档案、授权证书和聚合签名等信息生成的区块构成。医疗机构私有链上区块的一个交易数据由产生者医疗机构的身份 $I_{D_{HI}}$、患者个人健康档案信息 m_{PHR} 的签名 σ_B 和授权证书 w_{BP} 构成;第二个交易数据由主治医生 A_D 的 I_{D_A}、聚合签名 σ 和医生所在医疗机构的身份 $I_{D_{HI}}$ 构成。医疗机构将会生成不同的包含患者信息的区块,生成的区块将以时间为顺序,构成医疗机构私有链。

家庭私有链:就诊结束后,患者收到由代理签名者发送的聚合签名等信息,该信息在家庭私有链中生成新的区块,该区块的数据结构由产生者患者的身份 I_{D_P}、聚合签名 σ 和所就诊的医疗机构的身份 $I_{D_{HI}}$ 构成。家庭私有链中,所就诊的家庭成员作为区块的产生者,生成的区块以时间为顺序构成家庭私有链。

其中,块产生者的签名有助于追踪、时间戳显示块的生成时间,授权证书 w_{BP} 由参与授权的双方身份 I_D、代理权限 A 和代理期限 T 等信息构成,明确了两方间的交易规则,保护双方利益,代理签名私钥 x'_p 由患者生成,供代理签名者使用。

1.2　系统模型

系统中主要包括患者、代理签名者、医疗机构、主治医生、检查医生,模型如图 2 所示。

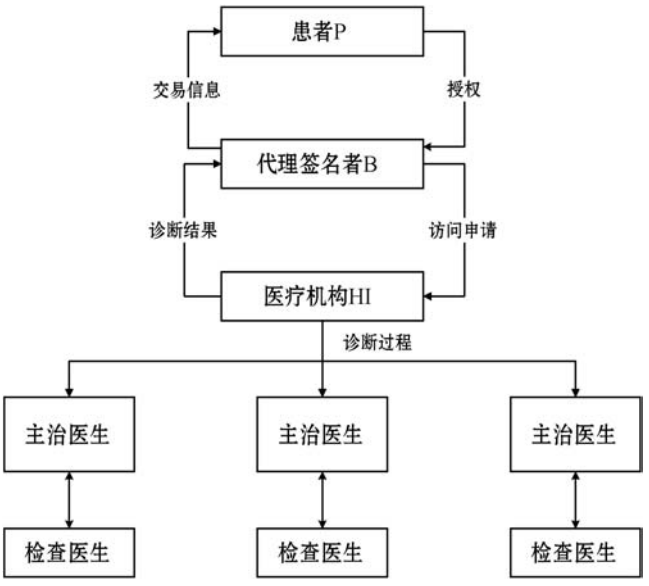

图 2　系统模型

患者、代理签名者、医疗机构、主治医生、检查医生都会生成各自的公私钥对。患者将自己的健康档案进行授权代理。使代理签名者拥有一定期限的患者个人健康档案的安全访问的权限,保证患者本人权益。授权成功后,代理签名者有权利代替授权人行使访问决定权,有权利查看患者的个人健康档案,不拥有增添和修改权。

患者需要就诊时,代理签名者向医疗机构发送访问申请,以保证双方信息真实可信,申请成功后,医疗机构和主治医生可获得该患者的相关信息。

患者就诊时,主治医生对其进行诊断,患者进行项目检查,检查医生将得出检查结果发送给主治医生,主治医生根据检查结果得出诊断结果,并将患者的检查结果和诊断结果提交至医疗机构。

医疗机构收到信息后,将该诊断结果发送给代理签名者,代理签名者收到信息验证无误后,将该交易信息发送给患者,患者收到信息后将其存储,此过程完成。

2　患者可授权的健康档案安全访问方法

2.1　方案模型

方案分为初始化阶段和访问阶段。

1) 方案初始化阶段包括代理授权、数据存储和身份认证,如图 3 所示。

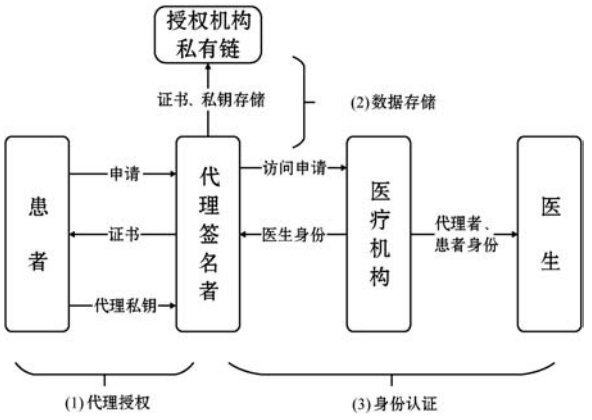

图 3 初始化阶段

(1) 代理授权。患者有控制访问权,假设患者由于某些不可控因素,需要将控制访问权限授权给代理签名者。首先患者向代理签名者发送申请,验证成功后,患者与代理签名者共同产生一个包含双方身份、代理权限、代理期限等信息的授权证书 w_{BP}。患者产生授权证书后将计算出来的代理签名私钥 x'_p 发送给代理签名者。代理签名者验证无误,代理授权完成。

(2) 数据存储。授权成功后,代理签名者将授权证书 w_{BP} 及生成的代理签名私钥 x'_p 递交至授权机构,授权机构私有链中节点验证成功后,将该交易数据存储。

(3) 身份认证。患者需要就诊前,代理签名者向医疗机构发送访问申请,申请通过后医疗机构向代理签名者提供主治医生(Attending Doctor)的身份信息 I_{D_A},同时向该主治医生发送就诊患者(Patient)和代理签名者的身份信息 I_{D_P}、I_{D_B}。代理签名者获得主治医生的 I_{D_A},主治医生得到患者和代理签名者的身份信息,认证完成。

2) 方案访问阶段包括档案签名、信息验证、诊断生成和信息存储,如图 4 所示。

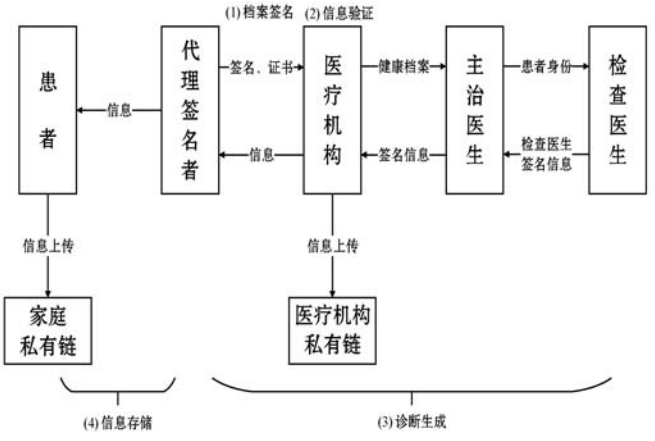

图 4 方案访问

(1) 档案签名。代理签名者将患者的个人健康档案签名,保证患者个人健康档案真实,不存在伪造虚假的情况。

(2) 信息验证。代理签名者将已签名的患者个人健康档案 σ_B 和授权证书 w_{BP} 秘密发送给医疗机构,医疗机构对签名的患者个人健康档案 σ_B 和授权证书 w_{BP} 进行验证。

(3) 诊断生成。医生行使诊断权。主治医生 A_D 收到代理签名者签名的患者个人健康档案,主治医生 A_D 将患者身份 I_{D_P} 发送给检查医生 E_{D_i}。检查医生 E_{D_i} 将患者的检查结果签名后发送给主治医生,主治医生 A_D 收到后,生成自己的诊断结果签名,并将所有结果签名上传至医疗机构,在医疗机构验证医生签名结果,验证成功后将签名信息聚合生成聚合签名,医疗机构将签名的患者个人健康档案 σ_B、授权证书 w_{BP} 和生成的聚合签名上传到医疗机构私有链中,同时将该交易数据信息打包秘密发送给代理签名者。

(4) 信息存储。代理签名者验证医疗机构发送过来的交易数据信息,验证无误后将该交易数据信息发送给患者,患者上传至所属家庭私有链中。

2.2 方案设计

2.2.1 方案初始化

设 q 是一个大素数,定义 Z_q 上的椭圆曲线为 E。$(G,+)$ 为椭圆曲线 E 上的 n 阶加法循环群,其中:n 是一个大素数,G 的一个生成元为 P,Z_q 为模 q 的群。设 H_1、H_2、H_3 为三个安全抗碰撞的 Hash 函数,$H_1:\{0,1\}^* \times G \rightarrow Z_n^*$,$H_2:Z_q^* \times \{0,1\}^* \rightarrow G$,$H_3:Z_q^* \times \{0,1\}^* \times Z_n^* \rightarrow Z_n^*$;系统公开参数为 $\{n,G,P,H_1,H_2,H_3\}$。

1) 代理授权。设患者(patient)的私钥为 x_p($x_p \in Z_n^*$),对应公钥为 $Q_p = x_p P$,patient 的身份为 I_{D_P}($I_{D_P} \in \{0,1\}^*$);B 为代理签名者,私钥为 x_B($x_B \in Z_n^*$),对应公钥为 $Q_B = x_B P$,代理签名者 B 的身份为 I_{D_B}($I_{D_B} \in \{0,1\}^*$)。patient 健康档案信息 m_{PHR}($m_{PHR} \in \{0,1\}^*$)中包括与其健康相关的信息。

patient:选择随机数 r_1($r_1 \in Z_n^*$),计算 $R_1 = r_1 Q_P$,patient 将 R_1 秘密发送给代理签名者 B。

代理签名者 B:收到 R_1 后,计算 $Y_1 = x_B R_1$,代理签名者 B 将 Y_1 秘密发送给 patient。

patient:收到 Y_1 后,验证等式 $r_1 x_P Q_B = Y_1$,是否成立。

若等式验证不成立,则拒绝接受;若等式成立,代理签名者 B 和 patient 共同产生授权证书 w_{BP},授权证书 w_{BP} 包含双方身份、代理权限 A、代理期限 T 等信息,$w_{BP} = (I_{D_p} \| I_{D_B} \| A \| T)$,授权证书 $w_{BP} \in \{0,1\}^*$。

代理签名者 B 和 Patient 共同产生授权证书 w_{BP} 后:

patient:计算授权许可 $A_P = x_p Y_1, u_1 = H_1(w_{BP}, A_P)$, $x'_p = x_P(r_1 + u_1) \bmod n$。patient 将$(x'_p, u_1)$秘密发送给代理签名者 B。

代理签名者 B:收到(x'_p, u_1)后,验证 $x'_p Q_B = Y_1 + x_B u_1 Q_P$是否成立,若等式成立,$x'_p$即为代理签名私钥,对应的代理签名公钥为 $Q'_p = x'_p P$。

2)数据存储。代理签名者 B 将授权证书 w_{BP}和代理签名私钥 x'_p递交至授权机构,授权机构私有链上的节点验证该交易数据,若验证通过,则授权机构确认消息,并将该交易数据存储在它的私有链中。

3)身份认证。HI 为医疗机构,设其私钥为 x_{HI}, $x_{HI} \in Z_n^*$,对应公钥为 $Q_{HI} = x_{HI} P$。

代理签名者 B:选择随机数 $r_2(r_2 \in Z_n^*)$,计算$R_2 = r_2 P = (x_2, y_2)$, $U_2 = H_2(x_2, w_{BP})$,并将(R_2, U_2)秘密发送给医疗机构 HI。

医疗机构 HI:收到(R_2, U_2)后,选择随机数 $\alpha_2(\alpha_2 \in Z_n^*)$,计算 $Y_2 = \alpha_2 P, K_2 = (x_{HI} + \alpha_2) R_2$并将$(Y_2, K_2)$秘密发送给代理签名者 B。

代理签名者 B:收到(Y_2, K_2)后,计算 $S_2 = x'_P Y_2 + K_2 + U_2$,并将 S_2秘密发送给医疗机构 HI。

医疗机构 HI:收到 S_2后,验证 $S_2 = \alpha_2 Q'_P + K_2 + U_2$是否成立,若等式成立,则接受申请,并向代理签名者 B 发送主治医生 A_D的身份信息 $I_{D_A}, I_{D_A} \in \{0,1\}^*$,同时向该主治医生发送就诊患者和代理签名者的身份信息 I_{D_P}、I_{D_B}, I_{D_P}、$I_{D_B} \in \{0,1\}$;若不成立,则拒绝申请。

2.2.2　方案访问

1)档案签名。代理签名者 B 收到 patient 秘密发送过来的 patient 健康档案信息 m_{PHR}。

医疗机构 HI:选择随机数 $d_{HI}(d_{HI} \in Z_n^*)$,计算 $D_{HI} = d_{HI} P$,并将 D_{HI}秘密发送给代理签名者 B。

代理签名者 B:收到 m_{PHR}、D_{HI}后,选择随机数 d_B, $d_B \in Z_n^*$,计算 $D_B = d_B P = (x_3, y_3)$, $l_B = H_3(x_3, m_{PHR}, u_1)$, $V_B = l_B(d_B + x_B) D_{HI}$,代理签名者 B 公开 l_B,并将$(D_B、V_B)$发送给医疗机构 HI。

2)信息验证。代理签名者 B 将信息 m_{PHR}的签名 σ_B和授权证书 w_{BP}秘密发送给医疗机构,医疗机构收到$(D_B、V_B)$后,首先验证信息 m_{PHR}的签名 $\sigma_B = (D_B, V_B)$, $V_B = d_{HI} l_B(D_B + Q_B)$是否成立,则医疗机构确认消息;若有不成立,则拒绝该信息。

该签名验证不会公开验证,该签名具有验证权限,在医疗机构许可下,获得其许可权限的请求者,可以验证上述签名的正确性。

3)诊断生成。主治医生 A_D收到通过验证的代理签名者 B 签名的患者个人健康档案,查看健康档案后,主治医生 A_D把 patient 将做的检查项目秘密发送给代理签名者 B,并将 patient 的身份 I_{D_P}发送给检医生 E_{D_i}, $i \in [1,m]$(Examining Doctor)。主治医生 A_D的私钥为 $x_{A_D}, x_{A_D} \in Z_n^*$,对应公钥为 $Q_{A_D} = x_{A_D} P$;检查医生 E_{D_i}的私钥为 $x_{D_i}, x_{D_i} \in Z_n^*$, $i \in [1,m]$,对应公钥为$Q_{D_i} = x_{D_i} P$,检查医生 E_{D_i}的身份为 $I_{D_{D_i}}, I_{D_{D_i}} \in \{0,1\}$, $i \in [1,m]$。

(1)检查医生 E_{D_i}。

医疗机构 HI:将 D_B发送给检查医生 E_{D_i}。

检查医生 E_{D_i}生成 patient 检查项目结果为 $\delta_i, \delta_i \in \{0,1\}^*$, $i \in [1,m]$。

检查医生 E_{D_i}:收到 D_B后,选择随机数 $d_i, d_i \in Z_n^*$, $i \in [1,m]$。计算 $D_i = d_i P, l_i = H_1(\delta_i \| I_{D_{D_i}}, D_B + D_i)$, $V_i = U_2 + (d_i + x_{D_i} l_i) P, \sigma_i = (D_i, V_i)$, σ_i为检查医生 E_{D_i}的检查项目结果签名,各检查医生 E_{D_i}公开 D_i、l_i并将(U_2, V_i, D_B)发送给主治医生 A_D。

(2)主治医生 A_D。

主治医生 A_D收到检查医生 E_{D_i}的检查项目结果签名 $\sigma_i = (D_i, V_i)$和(U_2, D_B)后,生成 patient 诊断结果 $\delta_0, \delta_0 \in \{0,1\}^*$。

主治医生 A_D:选择随机数 $d_0, d_0 \in Z_n^*$,计算 $D_0 = d_0 P, l_0 = H_1(\delta_0 \| I_{D_A}, D_B + D_0)$, $V_0 = U_2 + (d_0 + x_{A_D} l_0) P, \sigma_0 = (D_0, V_0)$, σ_0为主治医生 A_D的诊断结果签名,主治医生 A_D公开 D_0、l_0。

主治医生 A_D将所有的检查项目结果签名及自己的诊断结果签名,$\sigma_0, \sigma_1, \cdots, \sigma_m$上传至医疗机构 HI,医疗机构 HI 收后,计算 $V = \sum_{i=0}^{m} V_i, D = \sum_{i=0}^{m} D_i$,生成对 patient 的诊断结果的聚合签名 $\sigma = (D, V)$。

医疗机构 HI 将签名的患者个人健康档案 σ_B、授权证书 w_{BP}、聚合签名 σ 和医疗机构身份 ID_{HI}以交易数据的形式,上传到医疗机构私有链中,同时将该交易数据信息打包秘密发送给代理签名者 B。

4)信息存储。代理签名者 B 收到打包的交易数据信息后,首先验证该交易信息中的聚合签名是否成立, $V = (m+1) U_2 + l_0 Q_{A_D} + \sum_{i=0}^{m} D_i + \sum_{i=1}^{m} l_i Q_{D_i}$,若等式成立,则验证收到的交易数据信息,若验证通过,则确认该交易数据信息并将其发送 patient,并公开信息 U_2,patient 收到后存储到 patient 所属家庭私有链中。

3 方案分析

3.1 正确性分析

定理 1 若代理授权是有效的,则有 $r_1 x_P Q_B = Y_1$ 成立。

证明 若代理授权正确,需证明 $r_1 x_P Q_B = Y_1$ 成立,即:

$$r_1 x_P Q_B = r_1 x_P x_B P = r_1 x_B x_P P = r_1 x_B Q_P = x_B r_1 Q_P = x_B R_1 = Y_1$$

等式 $r_1 x_P Q_B = Y_1$ 成立,所以代理授权有效。

定理 2 代理签名密钥 $x'_p = x_P(r_1 + u_1) \bmod n$ 如果是合法的,则有等式 $x'_p Q_B = Y_1 + x_B u_1 Q_{Pv}$ 成立。

证明 若代理签名密钥 $x'_{pv} = x_P(r_1 + u_1) \bmod n$ 正确,则有:

$$x'_p Q_B = x_p(r_1 + u_1) Q_B r_1 x_p Q_B + x_p u_1 Q_B = Y_1 + x_B u_1 Q_P$$

定理 3 若对医疗机构 HI 的申请通过,则满足 $S_2 = \alpha_2 Q'_P + K_2 + U_2$。

证明 $S_2 = x'_P Y_2 + K_2 + U_2 = x'_P \alpha_2 P + K_2 + U_2 = \alpha_2 Q'_P + K_2 + U_2$

定理 4 若签名 $\sigma_B = (D_B, V_B)$ 是正确的,则有等式 $V_B = d_{HI} l_B (D_B + Q_B)$ 成立。

证明 $V_B = l_B(d_B + x_B) D_{HI} = l_B(d_B P + x_B P) d_{HI} = d_{HI} l_B (D_B + Q_B)$

定理 5 如果聚合签名 $\sigma = (D, V)$ 合法,则等式 $V = (m+1)U_2 + l_0 Q_{A_D} + \sum_{i=0}^{m} D_i + \sum_{i=1}^{m} l_i Q_{D_i} (i \in [1,m])$ 成立。

证明

$$V = \sum_{i=0}^{m} V_i = V_0 + V_1 + \cdots + V_m =$$
$$U_2 + d_0 P + x_{A_D} l_0 P + U_2 + d_1 P + x_{D_1} l_1 P + \cdots + U_2 + d_m P + x_{D_m} l_m P =$$
$$U_2 + D_0 + l_0 x_{A_D} P + U_2 + D_1 + l_1 x_{D_1} P + \cdots + U_2 + D_m + l_m x_{D_m} P =$$
$$U_2 + D_0 + l_0 Q_{A_D} + U_2 + D_1 + l_1 Q_{D_1} + \cdots + U_2 + D_m + l_m Q_{D_m} =$$
$$l_0 Q_{A_D} + U_2 + U_2 + \cdots + U_2 + D_0 + D_1 + \cdots + D_m + l_1 Q_{D_1} + \cdots + l_m Q_{D_m} =$$
$$(m+1)U_2 + l_0 Q_{A_D} + \sum_{i=0}^{m} D_i + \sum_{i=1}^{m} l_i Q_{D_i}$$

3.2 安全性分析

3.2.1 数据安全与访问控制

区块链的特点能够保证存储在区块链中的数据不可更改,如出现被更改的情况,则攻击者必须具有全网百分之五十一的计算能力,因此数据无法被修改[20]。本文构建私有链上的新区块分别附有代理签名者和医生的签名,保证了数据的真实性、可追溯性。存储在区块链上的患者健康档案数据,只有经过患者或代理签名者的允许才能获取。因此,患者能够对其个人健康档案进行访问控制。

3.2.2 非抵赖性

定理 6 代理签名方案是安全的。如果有任意敌手 O_1,以不可忽略的优势 ε_1 攻破了该方案,则可以防止代理签名者的不可抵赖。即使敌手 O_1 持有被代理者私钥,都不能伪造代理签名者签名。

本文代理签名方案中代理签名者不可抵赖是基于 CDH(Computational Diff-Hellman)假设。

证明 假定存在一个敌手 O_1,它以不可忽略的优势 ε_1 为代理签名方案输出一个伪造签名,我们构造一个算法 C_1,打破 CDH 问题。给定 n、G、P、H_1、H_2、H_3、xP、$yP \in G$,其中 x、$y \in Z_n^*$ 未知,计算 $xyP \in G$。对于算法 C_1 描述如下。

1) 给定一个 CDH 问题,$p_{arams} = \{n, G, P, H_1, H_2, H_3, xP, yP, xyP \in G\}$。

2) 代理签名者公私钥询问:O_1 最多可以发出 q_B 个代理签名者密钥询问,给定代理签名者索引 j,C_1 为任一代理签名者 B_j,产生 $(sk_j = x_{B_j}, pk_j = Q_{B_j} = x_{B_j} P)$,并发送 (sk_j, pk_j) 给 O_1。

3) H 询问:O_1 能够在 q_H 时间内询问 H 预言机,访问记录结构为数组 (w_{BP}, u_1)、(m_{PHR}, u_1, l_B) 的列表,若 O_1 询问时,若列表中有记录则返回对应的值 u_1、l_B 给 O_1;否则算法 C_1 随机地选择 $u_1 \in Z_n^*$、$l_B \in Z_n^*$,返回给 O_1。

4) 计算:假设 $d_B = x$、$d_{HI} = y$,C_1 计算 $D_B = d_B P = xP$,$D_{HI} = d_{HI} P = yP$,并将其发送给 O_1。

5) 回答:敌手 O_1 在多项式时间内计算消息签名对 (D_B, V_B^*),并将其发送到 C_1。

6) C_1 验证签名是否有效:$V_B^* = d_{HI} l_B (D_B + Q_B)$。

如果 V_B^* 为有效签名,C_1 计算:

$$V_B^* = l_B(d_B + x_B) D_{HI} = l_B(x + x_B) yP = l_B xyP + l_B x_B yP$$
$$l_B xyP = V_B^* - l_B x_B yP$$
$$xyP = \frac{V_B^*}{l_B} - x_B yP$$

这意味着 C_1 可以以不可忽略的概率来解决 CDH 问题,这与任何算法都很难解决 CDH 问题的假设相矛盾,因此代理签名为不可抵赖的。

其他签名者的不可抵赖性的证明与上述相同,因此只写出一个不可抵赖性的证明过程。

3.2.3 不可伪造性

在签名方案中,攻击者 O_2 如若知道任意签名者的

私钥,即可解决 CDH 困难问题。

定理 7　在随机预言模型下,假设存在一个敌手 O_2以不可忽略的优势 ε_2攻破了该方案,记 q_{H_i}和 t_{H_i}分别为敌手 O_2询问 $H_i(i=1,2,3)$预言机的次数和一次询问所需时间,记 q_s和 t_s分别为签名询问次数和一次询问所需时间,则存在算法 C_2,以优势 ε'_2解决 CDH 问题[21]。

证明　敌手 O_2通过调用算法 C_2,在一个概率多项式时间内解决了 CDH 难题。假设给定 $aP\in G$ 和 $bP\in G$,计算 abP,其中 $a,b\in Z_n^*$ 未知。C_2维护四张列表 L_{11}、L_{12}、L_2、L_3分别保存对 H_1、H_2、H_3的询问,然后 C_2运行系统初始化算法,输出 $p_{\text{arams}}=\{n,G,P,H_1,H_2,H_3\}$ 并将其发送给敌手 O_2。敌手 O_2收到系统参数后,执行如下询问:

(1) H_1询问。C_2维护一个记录结构为数组(w_{BP},u_1)的列表 L_{11}。当 O_2发起询问时,若列表 L_{11}中有记录则返回对应的值 u_1给 O_2;否则 C_2随机地选择 $u_1\in Z_n^*$,返回给 O_2,同时将(w_{BP},u_1)记录到列表 L_{11}中。

C_2维护一个记录结构为数组$(\delta_i\parallel I_{D_{D_i}},D_B+D_i,l_i)$的列表 L_{12}。当 O_2发起询问时,若列表 L_{12}中有记录则返回对应的值 l_i给 O_2;否则 C_2随机地选择 $l_i\in Z_n$,返回给 O_2,同时将$(\delta_i\parallel I_{D_{D_i}},D_B+D_i,l_i)$记录到列表 L_{12}中。

(2) H_2询问。C_2维护一个记录结构为数组(w_{BP},f_1,U_2)的列表 L_2。当 O_2发起询问时,若列表 L_2中有记录则返回对应的值 U_2给 O_2;否则,C_2随机选择 $f_1\in Z_n^*$,计算 $U_2=f_1aP$,将 U_2返回给 O_2同时将$(w_{\text{BP}},f_1,U_2=f_1aP)$记录到列表 L_2中。

(3) H_3询问。O_2维护一个记录结构为数组$(m_{\text{PHR}},u_1,l_{\text{B}})$的列表 L_3。当 O_2发起询问时,若列表 L_3中有记录则返回对应的值 l_{B}给 O_2;否则 O_2随机地选择 $l_{\text{B}}\in Z_n^*$,返回给 O_2,同时将$(m_{\text{PHR}},u_1,l_{\text{B}})$记录到列表 L_3中。

(4) 签名询问。$\delta_i(\delta_i\in\{0,1\}^*,i\in[1,m])$签名询问和 $\delta_0(\delta_0\in\{0,1\}^*)$签名询问相同,因此只写出一个签名询问过程。

当进行 $\delta_i(\delta_i\in\{0,1\}^*,i\in[1,m])$签名询问时:

C_2调出列表 L_{11}、L_{12}、L_2、L_3,随机选择 $d_i(d_i\in Z_n^*)$,计算 $D_i=d_iP$,$l_i=H_1(\delta_i\parallel I_{D_{D_i}},D_{\text{B}}+D_i)$,$V_i=U_2+(d_i+x_{D_i}l_i)P$,返回给 O_2,容易验证 O_2返回的签名满足验证等式 $V_i=f_1aP+(D_i+l_iQ_{D_i})$。

因此,有签名验证等式 $V_i^*=f_1aP+(D_i+l_iQ_{D_i})$ 成立,所以:

$$V_i^*=f_1aP+(D_i+l_iQ_{D_i})=f_1aP+d_iP+l_ix_{D_i}P$$

$$f_1aP=V_i^*-(d_i+l_ix_{D_i})P$$

$$abP=\frac{V_i^*-(d_i+l_ix_{D_i})}{f_1}bP$$

因此 C_2成功地计算出 $abP=\dfrac{V_i^*-(d_i+l_ix_{D_i})}{f_1}bP$,并输出$\dfrac{V_i^*-(d_i+l_ix_{D_i})}{f_1}bP$ 作为 CDH 问题的一个实例解答。

根据定理 7,针对攻击者,在随机预言模型以及 CDH 困难问题假设下,本文方案是存在性不可伪造的。

4　效率分析

4.1　功能性分析

本文与文献[20,22-26]进行了功能性对比,其中文献[20,22-24]皆应用于医疗电子病历,而文献[25-26]的应用环境是云服务器。结果如表 1 所示,对比发现,文献[23-26]均为非区块链数据存储平台。文献[20,22,25-26]中方案构造均为双线性映射,而文献[24]使用椭圆曲线的方法。文献[25-26]使用双线性映射构建代理重加密方案。表 2 中文献所提及方案均满足方案的访问控制和隐私保护,通过与以上方案的对比,表明本文方案在功能性上具有一定的优势。

表 1　功能性比对

功能特性	文献[20]	文献[22]	文献[23]	文献[24]	文献[25]	文献[26]	本文
区块链	√	√	×	×	×	×	√
访问控制	√	√	√	√	√	√	√
隐私保护	√	√	√	√	√	√	√
代理授权	无	无	无	无	代理重加密	代理重加密	有
加密方案	双线性对	双线性对	无	椭圆曲线	双线性对	双线性对	椭圆曲线

4.2　方案效率分析

表 2 中,T_{P}表示双线性配对运算的时间,T_{n}表示乘法运算的时间,T_{H}表示哈希运算的时间。可以看出,本文方案相对于文献[27]在代理授权阶段,本文比文献[27]的计算稍高,但在代理签名和聚合签名阶段本文比文献[27]的计算低。两方案整体相比,本文方案计算低于文献[27]且椭圆曲线运算效率大于双线性映射。

表 2　效率比对

方案	代理授权	代理签名	聚合签名
文献[27]	$3T_{\text{m}}+T_{\text{H}}$	$4T_{\text{m}}+3T_{\text{H}}$	$2T_{\text{P}}+3T_{\text{m}}+T_{\text{H}}$
本文方案	$4T_{\text{m}}+T_{\text{H}}$	$4T_{\text{m}}+T_{\text{H}}$	$2T_{\text{m}}+T_{\text{H}}$

5 结 语

本文提出一种基于区块链的可代理健康档案安全访问方案,在患者处于某些特殊情况下,可以将自己健康档案的访问权限授予给第三方。该方案分为初始化阶段和访问阶段。初始化阶段包括代理授权、数据存储和身份认证等过程。在该阶段中,患者将其个人健康档案的访问权限授予代理签名者,相关的授权信息存储在授权机构私有链中,同时代理签名者与医疗机构间进行身份认证,以保证健康档案信息的安全性。访问阶段包括档案签名、信息验证、诊断生成和信息存储等过程。在访问阶段,代理签名者需先将患者的个人健康档案进行签名,保证患者个人档案的真实性;医疗机构收到代理签名者发送的签名信息,并验证其正确性,确认无误后,将其发送给医生;医生对该患者作出相应的诊断,对诊断的结果进行签名,然后上传至医疗机构,医疗机构产生一个针对该患者的聚合签名,同时将该信息存储至医疗机构私有链中;代理签名者收到医疗机构发送的打包信息并验证,然后发送给患者,患者将收到的信息存储到家庭私有链中。该方案实现了数据安全、访问控制和隐私保护的安全目标,满足不可抵赖性,且具有较强的功能性及较低的运算量。在随机预言模型以及 CDH 困难问题假设下,本文方案是存在性不可伪造的。

参 考 文 献

[1] Liu P T S. Medical record system using blockchain, big data and tokenization[C]//18th International Conference on Security Information and Communications Security, 2016: 254 - 261.

[2] Yue X, Wang H J, Jin D W, et al. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control[J]. Journal of Medical Systems, 2016, 40: 218.

[3] Hölbl M, Kompara M, Kamišalić A, et al. A systematic review of the use of blockchain in healthcare[J]. Symmetry, 2018, 10(10): 470.

[4] Beinke J H, Fitte C, Teuteberg F. Towards a stakeholder-oriented blockchain-based architecture for electronic health records: Design science research study[J]. Journal of Medical Internet Research, 2019, 21(10): e13585.

[5] Alex R, Costa C A, Righi R D, et al. Analyzing the performance of a blockchain-based personal health record implementation[J]. Journal of Biomedical Informatics, 2019, 92: 1 - 9.

[6] Agbo C, Mahmoud Q H. Blockchain in healthcare: Opportunities, challenges, and possible solutions[J]. International Journal of Healthcare Information Systems and Informatics, 2020, 15(3): 82 - 97.

[7] Tanwar S, Parekh K, Evans R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications[J]. Journal of Information Security and Applications, 2020, 50: 102407.

[8] Chen T L, Liao Y T, Chang Y F, et al. Security approach to controlling access to personal health records in healthcare service[J]. Security & Communication Networks, 2016, 9(7): 652 - 666.

[9] Pussewalage H S G, Oleshchuk V A. Attribute based access control scheme with controlled access delegation for collaborative E-health environments[J]. Journal of Information Security and Applications, 2017, 37: 50 - 64.

[10] Marwan M, Kartit A, Ouahmane H. A cloud based solution for collaborative and secure sharing of medical data[J]. International Journal of Enterprise Information Systems, 2018, 14(3): 128 - 145.

[11] Tang W J, Ren J, Zhang K, et al. Efficient and privacy-preserving fog-assisted health data sharing scheme[J]. ACM Transactions on Intelligent Systems and Technology, 2019, 10(6): 1 - 23.

[12] Edemacu K, Jang B, Kim J W. Collaborative eHealth privacy and security: An access control with attribute revocation based on OBDD access structure[J]. IEEE Journal of Biomedical and Health Informatics, 2020, 24(10): 2960 - 2972.

[13] Azaria A, Ekblaw A, Vieira T, et al. MedRec: Using blockchain for medical data access and permission management[C]//2nd International Conference on Open and Big Data, 2016: 25 - 30.

[14] Dubovitskaya A, Xu Z G, Ryu S, et al. Secure and trustable electronic medical records sharing using blockchain[J]. AMIA Annual Symposium Proceedings, 2017, 8: 650 - 659.

[15] Xia Q, Sifah E B, Smahi A, et al. BBDS: Blockchain-based data sharing for electronic medical records in cloud environments[J]. Information, 2017, 8(2): 44.

[16] Dagher G, Mohler J, Milojkovic M, et al. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology[J]. Sustainable Cities & Society, 2018, 39: 283 - 297.

[17] Thwin T, Vasupongayya S. Blockchain based secret-data sharing model for personal health record system[C]//5th International Conference on Advanced Informatics: Concept Theory and Applications, 2018: 196 - 201.

[18] Nagasubramanian G, Sakthivel R K, Patan R, et al. Securing E-health records using keyless signature infrastructure blockchain technology in the cloud[J]. Neural Computing and Applications, 2018, 32: 639 - 647.

(下转第 335 页)

在实现投诉举报信息机密性、不可传递性的同时,还有效地保护了举报者的身份信息,并且利用区块链中的保证金思想在一定程度上约束了举报行为,节省了社会资源。因此,本方案已满足了文初提到的一个良好的投诉举报系统所应具备的几个功能,并通过对其进行六个方面的分析后证明,此方案正确、安全而且可行。

参 考 文 献

[1] 马红军. 受理投诉举报的重要遵循—《社会组织登记管理机关受理投诉举报办法(试行)》解读[J]. 中国社会组织,2016(16):34 – 35.

[2] 苗付友,王行甫,苗辉,等. 一种支持悬赏的匿名电子举报方案[J]. 电子学报,2008,36(2):320 – 324.

[3] 王化群,于红,吕显强,等. 一种支持悬赏的匿名电子举报方案的安全性分析及设计[J]. 电子学报,2009,37(8):1826 – 1829.

[4] Wu L, Hu D. Strong designated verifier ID-based threshold ring signature scheme[J]. International Journal of Applied Mathematics and Statistics,2013,41(11):222 – 229.

[5] 张瑞丽,李顺东. 一种新的基于身份的匿名电子举报方案[J]. 计算机应用与软件,2015,32(2):288 – 290,294.

[6] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [EB/OL]. [2020 – 06 – 29]. https://bitcoin. org/bitcoin. pdf.

[7] Kiyomoto S, Rahman M S, Basu A. On blockchain-based anonymized dataset distribution platform[C]//15th International Conference on Software Engineering Research, Management and Applications,2017:85 – 92.

[8] Sasson E B, Chiesa A, Garman C, et al. Zerocash: Decentralized anonymous payments from bitcoin[C]//IEEE Symposium on Security and Privacy,2014:459 – 474.

[9] 高建平. 基于 CDH 的模糊身份多方加密方案[J]. 网络安全技术与应用,2020(1):45 – 47.

[10] Tapscott D, Tapscott A. Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world[M]. New York: Portfolio,2016:72,83,101,127.

[11] Lind J, Naor O, Eyal I, et al. Teechain: Reducing storage costs on the blockchain with offline payment channels[C]//11th ACM International Systems and Storage Conference, 2018:125.

[12] Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM,1983,26(1):96 – 99.

[13] Chaum D, Heyst E V. Group signatures[C]//Workshop on the Theory and Application of Cryptographic Techniques, 1991:257 – 265.

[14] Enge A. Bilinear pairings on elliptic curves[EB]. arXiv: 1301.5520v1,2013.

[15] Boneh D, Franklin M. Identity-based encryption from Weil pairing[C]//Annual International Cryptology Conference, 2001:213 – 229.

[16] Crampton J. Specifying and enforcing constraints in role-based access control[C]//8th ACM Symposium on Access Control Models and Technologies,2003:43 – 50.

[17] Merkle R C. A certified digital signature[C]//Conference on the Theory and Application of Cryptology,2001,218 – 238.

[18] Herranz J, Sáez G. New identity-based ring signature schemes [C]//6th International Conference on Information and Communications Security,2004:27 – 39.

[19] Castro P, Melnik S, Adya A. ADO. NET entity framework: Raising the level of abstraction in data programming[C]//ACM SIGMOD International Conference on Management of Data,2007:1070 – 1072.

[20] Blakeley J A, Campbell D, Muralidhar S, et al. The ADO. NET entity framework: Making the conceptual level real[J]. ACM SIGMOD Record,2006,35(4):32 – 39.

(上接第 322 页)

[19] Arunkumar B, Kousalya G. Blockchain-based decentralized and secure lightweight E-health system for electronic health records[C]//5th Intelligent Systems, Technologies and Applications,2020:273 – 289.

[20] 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 – 2039.

[21] 左黎明,周庆,陈兰兰. 一种可证安全高效无证书短签名方案[J]. 计算机工程,2019,45(6):193 – 198.

[22] Zhang A Q, Lin X D. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain [J]. Journal of Medical Systems,2018,42(8):140 – 158.

[23] 袁勇,倪晓春,曾帅,等. 区块链共识算法的发展现状与展望[J]. 自动化学报,2018,44(11):2011 – 2022.

[24] Zhang J, Xue N, Huang X. A secure system for pervasive social network-based healthcare[J]. IEEE Access,2016,4: 9239 – 9250.

[25] 韩笑,曾琦,曹永明. 一种有效的带关键字搜索的代理重加密方案[J]. 计算机与现代化,2019,283(3):117 – 121.

[26] 郭丽峰,李婷. 改进的带关键字搜索的代理重加密方案[J]. 山西大学学报(自然科学版),2016,39(3):434 – 441.

[27] 张青,何为,戴阔斌,等. 一种可证明安全的代理聚合签名方案[J]. 武汉大学学报(理学版),2018,64(5):415 – 422.