计算机科学
COMPUTER SCIENCE

基于可编辑医疗联盟链的数据安全管理方案

谭婧颀，薛凌妍，黄海平，陈龙，李逸轩

引用本文

谭婧颀，薛凌妍，黄海平，陈龙，李逸轩. 基于可编辑医疗联盟链的数据安全管理方案[J]. 计算机科学, 2024, 51(6A): 240400056-8.

TAN Jingqi, XUE Lingyan, HUANG Haiping, CHEN Long, LI Yixuan. Data Security Management Scheme Based on Editable Medical Consortium Chain [J]. Computer Science, 2024, 51(6A): 240400056-8.

相似文章推荐（请使用火狐或 IE 浏览器查看文章）

Similar articles recommended (Please use Firefox or IE to view the article)

基于联盟链的跨组织数据交换操作一致性模型

Operational Consistency Model Based on Consortium Blockchain for Inter-organizational Data Exchange

计算机科学, 2024, 51(6A): 230800145-9. https://doi.org/10.11896/jsjkx.230800145

基于多用户变色龙哈希的可修正联盟链方案设计

New Design of Redactable Consortium Blockchain Scheme Based on Multi-user Chameleon Hash

计算机科学, 2024, 51(6A): 230600004-6. https://doi.org/10.11896/jsjkx.230600004

跨域数据管理

Cross-domain Data Management

计算机科学, 2024, 51(1): 4-12. https://doi.org/10.11896/jsjkx.yg20240102

用户公平保障的边缘服务缓存与任务卸载算法

Fairness-aware Service Caching and Task Offloading with Cooperative Mobile Edge Computing

计算机科学, 2023, 50(11A): 230200095-8. https://doi.org/10.11896/jsjkx.230200095

基于可跟踪环签名的拜占庭容错共识算法

Byzantine Fault Tolerant Consensus Algorithm Based on Traceable Ring Signature

计算机科学, 2023, 50(6A): 220300100-7. https://doi.org/10.11896/jsjkx.220300100

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.240400056

基于可编辑医疗联盟链的数据安全管理方案

谭婧颀[1]　薛凌妍[1]　黄海平[1,2]　陈　龙[1,2]　李逸轩[1]
1 南京邮电大学计算机学院　南京 210023
2 江苏省无线传感网高技术研究重点实验室　南京 210023
(b21031405@njupt.edu.cn)

摘　要　医疗数据的安全管理是确保患者隐私安全、有效开展医学诊疗与相关研究的关键。然而,现有的医疗数据管理方案大多存在透明度低、共享性差和无法保证患者隐私数据安全性的问题。通过设计一种“主-侧”链结构的可编辑区块链模型,提出了面向医疗联盟链的安全、可追责的医疗数据管理方案。该模型主链保存患者电子病历的最新信息,侧链记录历史修改证明,实现了数据管理的透明性和可追责性。引入变色龙哈希函数、秘密共享和可验证签名技术,只有通过验证的医疗机构的系统管理员才能够参与构建完整陷门,确保了医疗数据修改过程的正确性与安全性。经过安全性分析和相关实验模拟,该方案在计算开销、通信负载方面的性能较好,且在存储开销方面存在优势,表明了该方案的有效性和可行性。

关键词:数据管理;联盟链;可编辑区块链;秘密共享;数字签名
中图分类号　TP393.08

Data Security Management Scheme Based on Editable Medical Consortium Chain

TAN Jingqi[1],XUE Lingyan[1],HUANG Haiping[1,2],CHEN Long[1,2] and LI Yixuan[1]
1 School of Computer Science,Nanjing University of Posts and Telecommunications,Nanjing 210023,China
2 Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks,Nanjing 210023,China

Abstract　Secure management of medical data is crucial for ensuring the security of patient privacy and effectively conducting medical treatments and related research. However,most existing medical data management solutions have the problems of low transparency,inadequate sharing and fail to secure patient privacy. By designing an editable blockchain model with a “main-side” chain structure,a secure and accountable healthcare data management scheme for healthcare consortium chain is proposed. Its main chain stores current information about the patient's electronic medical record,while the side chain records historical proof of modification,enabling the transparency and traceability of data management. Introducing chameleon hash function,secret sharing and verifiable signature technology,only verified system administrators of healthcare organizations are able to construct the complete trapdoor,which ensures the correctness and security of the medical data modification process. Security analysis and related experiment simulation show that,the proposed scheme performs well in computational overhead and communication load,as well as storage efficiency,which demonstrates its effectiveness and feasibility.

Keywords　Data management,Consortium chain,Editable blockchain,Secret sharing,Digital signature

1　引言

医疗数据指在医学诊疗过程中和医学相关研究中涉及的所有数据,如电子病历,这类数据产生快、种类多、总量大,通常包含与患者健康状况相关的隐私信息,因而需要被严格管理。如今,医疗数据的管理现状面临诸多挑战。首先,患者的医疗数据仍然由各个医疗机构独立掌握,无法确保患者的隐私安全,存在隐私泄露的风险。其次,现有的医疗数据管理方案的透明度较低,患者无法知道自己数据的存储与维护过程,也无法控制数据的分享权限。此外,医疗机构存储的数据可能会因人为失误或者系统故障等而出现错误操作或丢失,且难以修正或找回。各医疗机构间的不信任进一步阻碍了健康数据的共享与同步[1],导致病人在不同医疗机构就诊时需要重复检查,造成医疗资源的浪费,并降低诊疗效率。因此,迫切需要一种安全、可靠的医疗数据管理方案。

区块链技术自首次被提出以来,因具有去中心化、不可篡改、可追溯以及可编程性等优良特性而被广泛应用到金融、物流、医疗、审计和政务等诸多领域,显著提高了整个行业的效率和水平。在医疗数据管理方面,区块链技术不仅能够保证病人健康数据的安全性,也能够实现相关数据在各医疗机构间的共享等功能,为医疗数据管理提供了一种创新的解决方案。然而,区块链技术的不可篡改性虽然确保了链上历史数据的完整可靠,但给医疗数据管理带来了挑战。一方面,《通用数据保护条例》赋予了患者更正和删除自己的健康数据的

基金项目:国家自然科学基金(62072252);江苏省研究生科研实践创新计划资助项目(KYCX210790,KYCX23_1086,CX10284)
This work was supported by the National Natural Science Foundation of China(62072252) and Postgraduate Research & Practice Innovation Program of Jiangsu Province(KYCX210790,KYCX23_1086,CX10284).
通信作者:黄海平(hhp@njupt.edu.cn)

权利[2]，而区块链的固有特性则限制了这类操作。另一方面，不可避免的人为失误导致错误的医疗数据被记录在链上，而这些数据难以被更改或删除，制约了区块链医疗数据管理系统的实际使用。为此，Ateniese 等[3]于 2017 年提出了一种可编辑区块链方案，其利用变色龙哈希函数允许在特定条件下修改链上的错误数据。在该方案的基础上，学术界相继提出了许多可编辑区块链方案。根据管理陷门的方式可分为中心化与去中心化两类[4]。具体而言，在中心化的可编辑区块链方案中，单一节点掌控变色龙哈希函数的完整陷门，这类模型容易因节点遭受攻击或恶意行为而破坏系统的安全性。在医疗联盟链中，这类方案可能降低系统效率。而去中心化的可编辑区块链方案通常将完整陷门分散给多个节点，一定程度上提高了区块链系统的安全性。但在陷门恢复过程中，可能存在攻击者在通信过程中伪造、篡改陷门碎片，或恶意节点提供错误的陷门碎片，进而导致陷门无法重构。此外，现有的可编辑区块链方案通常未存储历史修改过程，导致无法进行追溯或审计。综合上述分析，可编辑区块链为医疗数据管理提供了新的思路，但现有方案仍未能完全解决医疗数据管理的挑战。

针对上述挑战，本文的主要贡献如下：

1)设计了一种“主-侧”链结构的可编辑联盟链模型，确保医疗数据管理的透明性和可追溯性。在该模型中，患者的电子病历数据存储于主链上，而相关的历史修改证明被记录在主链对应的侧链区块中，主链区块中始终保存最新的病历数据信息，依据侧链中记录的历史数据变更信息实现了对数据修改行为的可追责性。

2)基于上述模型，提出了一种安全、可追责的医疗数据管理方案。联盟链中各医疗机构预选出的系统管理员分别持有变色龙哈希函数的主陷门碎片，并共同生成相对应的公钥，有助于区块链状态的同步。当主链区块发生交易修改时，只有通过签名验证的碎片可以参与完整陷门的构建，从而确保管理员能够正确修改医疗数据。

3)针对所提方案，给出了详细的安全性分析，并通过实验模拟和研究对比评估了方案在计算开销、通信负载，以及存储开销方面的性能，证明了本方案的有效性和可行性。

2 相关工作

随着科技进步，国内外许多学者利用区块链技术提出了多种医疗数据管理方案。例如，Azaria 等[5]提出了一种新型去中心化记录与管理电子病历的 MedRec 系统，该系统在保证病人隐私的同时，也让病人能够随时访问自己的医疗数据。Xue 等[6]设计了一个医疗数据共享模型，通过改进共识机制实现安全便捷的数据共享，从而解决了各医疗机构间数据共享的难题。Zhang 等[7]运用实用拜占庭容错算法提出 Medical Chain 联盟式医疗区块链系统，该系统能够有效防止链上医疗数据被泄露与篡改，并且实现了病人医疗数据信息在各医疗机构间的共享。然而，上述研究均没有考虑链上数据不可更改的限制，区块链上错误的医疗数据若无法更改，或大量陈旧的医疗数据无法更新，会严重限制系统的长期可用性。因此，基于可编辑区块链技术设计的医疗数据管理方案更具有实用性与应用潜力。

近年来，学术界利用可编辑区块链技术提出了许多数据管理方案。例如，Zhao 等[8]对区块链编辑过程的可追责性进行研究，当编辑后的区块验证失败时，监管者可以对相关方追责，但该方案需要额外的领导者参与投票与选择编辑者，涉及多方计算，方案复杂度较高。Lv 等[9]设计了一种面向联盟链的可验证的区块链账本修改方案，该方案具有去中心化特性，即由所有权限节点共同生成变色龙哈希公钥与私钥，但提案节点只有在得到所有子私钥的情况下才可以恢复出系统私钥。Wang 等[10]为实现各医疗机构之间数据的共享与电子病历的更新，提出了一种可编辑电子病历的共享方案，同时基于决策双线性 Diffie-Hellman 假设证明了系统的安全性，但该方案忽略了电子病历修改记录的存储，无法实现可追责性。Marsalek 等[11]设计了一种能够编辑任意数据类型的区块链架构，打破了现有的可编辑区块链方案只支持编辑特定类型的存储数据的局限性，但每次修改后需要重复读取原始区块链数据，时间开销较大。Jia 等[12]提出的可编辑区块链采用了 RSA 累加器技术，解决了可编辑区块链中的可追溯性与区块一致性的问题。

基于可编辑区块链技术的研究持续推进，并已衍生出多种应用。如 Zhang 等[13]将可编辑区块链技术应用于工业物联网，提出了一种可信的工业数据管理方案，通过建立双区块链架构分离数据管理与区块链管理，提高了工业数据管理的安全性与可行性。Li 等[14]探索了可编辑区块链技术的潜力，提出了一种保护隐私的动态可搜索加密框架(DSE-RB)，该方案是一种保证加密数据可靠查询和更新的通用方案。这些研究表明了可编辑区块链技术在提升数据管理安全性方面的潜力。

3 方案设计

3.1 系统模型

如图 1 所示，本文设计了一种安全、可追责的分布式可编辑医疗联盟链系统，该系统包含 4 种实体：医生用户(U)、系统管理员(M)、可信第三方(TTP)，以及可编辑区块链(MBC)。其具体定义分别如下：

医生用户(U)：医生用户可以向区块链系统提交患者的医疗数据，并向其所在医疗机构的系统管理员发出修改病人电子病历请求，但不参与可编辑区块链的维护与链上信息的修改。

系统管理员(M)：每个医疗机构预先选定系统管理员，每位系统管理员持有自身相应的陷门碎片。他们主要负责恢复完整的陷门并修改链上交易，并生成修改的相关证明。

可信第三方(TTP)：可信第三方主要负责依据智能合约部署区块链系统，生成系统参数和完整陷门，并将陷门碎片分发给各医疗机构的系统管理员。

可编辑区块链(MBC)：可编辑区块链由主链和侧链构成，主链存储正确的且最新的患者电子病历数据，医疗相关的修改证明则被记录在主链对应的侧链区块中。

首先，可信第三方依据智能合约部署区块链系统并设定系统参数，同时生成系统完整陷门。然后，对陷门进行分片处理和备份，并分发给各医疗机构的系统管理员。

其次，各医疗机构系统管理员共同生成变色龙哈希函数的公钥。完成初始设置后，可信第三方将离线，由各医疗机构中的医生用户使用该系统来存储患者医疗数据，机构管理员

则可以修改主链数据并在侧链中记录历史数据的修改证明。特别地,该方案中仅各医疗机构预选出的唯一系统管理员持有系统陷门碎片,在需要修改患者的医疗数据时,满足陷门条件的其他机构管理员同意修改后,提出修改申请的系统管理员即可恢复系统完整密钥,完成数据修改,同时生成修改相关的证明,存储于修改后的主链区块对应的侧链区块中。

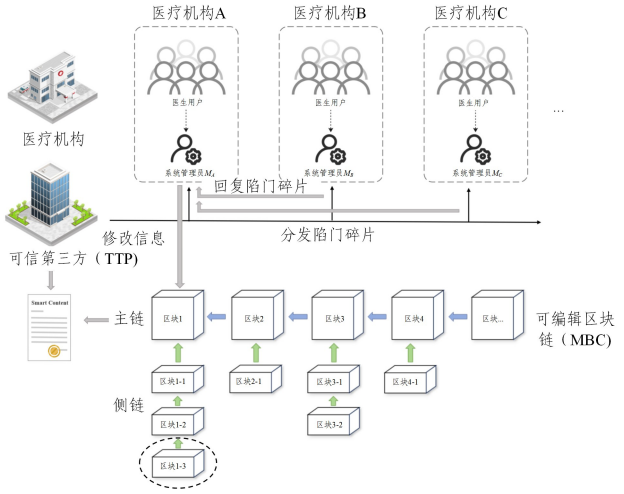

图 1　医疗数据管理系统模型

Fig. 1　Medical data management system model

3.2　方案设计

3.2.1　符号表

为了形式化描述所提方案,本文使用的重要符号及其相关说明如表 1 所列。

表 1　符号及其说明

Table 1　Symbols and their descriptions

符号	说明
M_i	第 i 位系统管理员
x_i	第 i 个系统陷门碎片
y_i	第 i 个系统公钥片段
T	完整陷门
m,m'	原始消息,新消息
r,r'	原始随机数,碰撞后的随机数
CH	变色龙哈希值
$PKey$	完整公钥

3.2.2　算法设计

本文所提方案包括 3 个阶段:区块链初始化、主链区块生成和医疗数据修改与验证。具体步骤如下。

1)区块链初始化阶段

该阶段完成区块链系统的初始化工作,主要包括生成系统公共参数与变色龙哈希函数完整陷门,分发陷门碎片以及系统管理员共同生成完整公钥。首先,由可信第三方 TTP 调用 SetUp 算法生成必要的系统公共参数 pp,来初始化可编辑区块链主链。然后调用 TrapdoorGen 算法生成系统完整陷门 T,同时对陷门进行分片处理,并将陷门碎片发送给各医疗机构预先选定的 n 个系统管理员$\{M_A,M_B,M_C,\cdots,M_n\}$。此外,所有系统管理员由 PKeyGen 算法共同生成变色龙哈希函数的公钥。

(1)SetUp

输入安全参数 λ,生成系统公共参数 $pp=\{p,q,g\}$,其中 p,q 满足 $q|(p-1)$,g 是 Z_p^* 的生成元,即 $g^q\equiv1(\mathrm{mod}\ p)$。

(2)TrapdoorGen

对于各医疗机构的 n 位系统管理员$\{M_A,M_B,M_C,\cdots,M_n\}$,TTP 选择 n 个互不相同的随机数$\{x_1,x_2,x_3,\cdots,x_n\}$作为对应的陷门碎片,其中 $x_i\in Z_q^*$ $(i\in[1,n])$。依据陷门碎片,可以得出该方案中变色龙哈希函数的完整陷门为:

$$T=\sum_{i=1}^{n}x_i \tag{1}$$

在该算法中,可信第三方以秘密共享的方式分发陷门碎片,即选取阈值 t,在有限域 Z_q^* 上构造如下 $t-1$ 次多项式:

$$f(x)=s+a_1x+\cdots+a_{t-1}x^{t-1} \tag{2}$$

其中,常数项 s 即为系统完整陷门 T,随机系数 $a_1,a_2,\cdots,a_{t-1}$ 满足 $a_i\in Z_q^*$ $(i\in[1,t-1])$。

对于每个陷门碎片$\{x_1,x_2,x_3,\cdots,x_n\}$,TTP 计算对应的 $f(x_i)$,并为所有系统管理员分别生成特定身份标识 P_i^{id},将 $(x_i,f(x_i),P_i^{\mathrm{id}})$分别发送给各医疗机构的系统管理员。

(3)PKeyGen

各医疗机构系统管理员调用 PKeyGen 算法共同生成变色龙哈希函数的公钥,PKeyGen 算法流程如下:

Step1　第一位系统管理员 M_A 利用自身陷门碎片 x_1 生成自己的公钥片段 $y_1=g^{x_1}(\mathrm{mod}\ p)$,并将 y_1 发送给第二位系统管理员 M_B。

Step2　第二位系统管理员 M_B 接收到 y_1 后,再利用自身拥有的陷门碎片 x_2 生成自己的公钥片段 $y_2=g^{x_2}(\mathrm{mod}\ p)$,$M_B$ 计算出公钥片段 y_2 与 y_1 的乘积 $y_1\cdot y_2=g^{x_1}\cdot g^{x_2}(\mathrm{mod}\ p)=g^{x_1+x_2}(\mathrm{mod}\ p)$,并将结果发送给第三位系统管理员 M_C。以此类推,即在整个公钥片段的生成过程中,第 i 位系统管理员 M_i 生成第 i 个系统公钥片段 y_i 的计算式如下:

$$y_i=g^{x_i}(\mathrm{mod}\ p) \tag{3}$$

而第 i 位系统管理员 M_i 接收到的消息为前 $i-1$ 位系统管理员公钥碎片的总乘积,即:

$$\prod_{j=0}^{i-1}y_j=g^{\sum_{j=0}^{i-1}x_j}(\mathrm{mod}\ p) \tag{4}$$

Step3　最后一位系统管理员 M_n 生成公钥片段 y_n 后,可获得系统的完整公钥 $PKey$,即:

$$PKey=\prod_{i=1}^{n}y_n=g^{\sum_{i=1}^{n}x_i}(\mathrm{mod}\ p) \tag{5}$$

M_n 将完整公钥 $PKey$ 发送给其余所有系统管理员,$PKey$ 成为该可编辑区块链上的公共参数。

2)主链区块生成阶段

区块链初始化完成后,医生用户(U)的患者的医疗数据加密存储于区块链主链上,给定消息 m、系统完整公钥 $PKey$ 和系统参数 p,q,系统管理员随机选择随机数 $r\in Z_q^*$,计算该消息的变色龙哈希值为:

$$CH=Hash(PKey,m,r)=g^mPKey^r(\mathrm{mod}\ p) \tag{6}$$

经过交易验证和共识后,由随机的系统管理员选择合法的交易进行打包,最后将区块连接到区块链主链上。

3)医疗数据修改与验证阶段

若区块链存储的患者的医疗数据发生错误或病人病情发生转变,则需要对区块链主链上存储的数据进行修改或更新。当某医疗机构的系统管理员 M_j 收到来自医生用户的修改请求时,其余系统管理员若同意修改,则将签名后的$(x_i,f(x_i))$发送给该系统管理员 M_j,系统管理员 M_j 收到后可以验证接收到的消息是否正确。

在获得任意 t 个合法的陷门碎片 x_i 与对应的 $f(x_i)$后,

提出修改请求的系统管理员 M_j 就可以调用 ReTrapdoor 算法恢复系统完整陷门，并用 Forge 算法修改原始电子病历信息。其余系统管理员收到消息后，执行 Verify 函数以验证 CH 与 m'，r' 是否匹配。具体算法描述如下：

Signature：当任意两个系统管理员进行信息传输时，接收方调用该算法验证签名的有效性，以确保消息未被篡改。设任意两名系统管理员 M_A 和 M_B 传递的消息为 n，即 $n=(x_i, f(x_i))$。算法具体流程为：

Step1 消息发出方进行签名

发出方 M_A 首先选择随机数 k，对消息 n 做下列计算：

$$\begin{aligned} u &= g^k \pmod p \\ h &= Hash(u,n) \\ s &= x_i h + k \pmod q \end{aligned} \tag{7}$$

则 M_A 可以计算得到其签名 $sig=(h,s,y_i)$，其中 y_i 为消息发出方自身的公钥碎片，即 $y_i=g^{x_i} \pmod p$，并将消息 n 与签名共同发送给信息接收方 M_B。

Step2 消息接收方进行验证

接收方 M_B 收到 (n,sig) 后，先计算 $u'=g^s y_i^{-h} \pmod p$，再计算 $Hash(u',n)$ 的值。若等式 $Hash(u',n)=h$ 成立，则表明该签名正确，该消息完整可靠；若等式不成立，则表明签名无效，即该消息已被恶意篡改。

ReTrapdoor：该算法基于陷门碎片生成完整陷门 T。当获取到任意至少 t 个合法的系统管理员的陷门碎片 x_i 与对应的 $f(x_i)$ 时，可以构造出 t 阶线性方程组，以获得 s。其中，t 阶线性方程组如式(8)所示：

$$\begin{cases} f(x_1)=s+a_1x_1+a_2x_1+\cdots+a_{t-1}x_1^{t-1} \\ f(x_2)=s+a_1x_2+a_2x_2+\cdots+a_{t-1}x_2^{t-1} \\ \cdots \\ f(x_t)=s+a_1x_t+a_2x_t+\cdots+a_{t-1}x_t^{t-1} \end{cases} \tag{8}$$

在上述方程组中，将 x_i 看作系数，假设系数矩阵为 $\boldsymbol{D}$，显然矩阵 $\boldsymbol{D}$ 是范德蒙德矩阵。而 $x_i(i\in[1,n])$ 取值均不相同，所以 $\det(\boldsymbol{D})\neq 0$，该线性方程组有唯一解，表明该指定系统管理员能够恢复完整陷门 T，实现对患者医疗数据的修改。

Forge：该算法能够将原始消息 m 修改为新消息 m'，而修改前后的变色龙哈希值 CH 保持不变。输入原始随机数 r、变色龙哈列值 CH、陷门 T 和新消息 m'，能够输出一个新随机数 r'，使固定的变色龙哈列值 CH 与 m'，r' 相匹配。即：$CH(m,r,PKey)=CH(m',r',PKey)$，其中新随机数 r' 可以由式(9)计算：

$$r'=(m-m')\cdot T^{-1}+r \pmod q \tag{9}$$

Verify：输入公钥 $PKey$、新可变参数 r'、新消息 m'、变色龙哈希值 CH，验证 CH 与 m'，r' 是否匹配。如果匹配，则输出 1，否则输出 0。

3.2.3 数据管理具体设计

图 2 给出了医疗数据管理的具体流程。当医生用户 U_A 认为区块链主链第 i 个区块的第 j 条消息需要修改时，首先在本地修改该条消息，然后向其所属医院的系统管理员 M_A 提出修改第 i 个区块的第 j 条消息的提案，由 M_A 将该提案广播给其余所有系统管理员。

其余系统管理员回复同意或反对并广播，同时同意修改消息的系统管理员将自身陷门碎片 x_i 回复给 M_A，而反对修改的管理员则不回复自身陷门碎片。

收到至少 t 个系统管理员的同意修改后，理论上 M_A 能够恢复系统完整陷门并执行 Forge 算法，获得关于新消息的新可变参数 r_j'。M_A 将 r_j' 广播给其余节点，其余节点接收到该消息后，执行验证函数 $Verify$，以验证 CH 与 m_j'，r_j' 是否匹配。若能够成功匹配，则更新自身本地区块信息。反之，若少于 t 个系统管理员同意修改，则 M_A 无法恢复系统完整陷门，进而无法在区块链上修改对应信息，表明医生用户 U_A 的请求被拒绝。

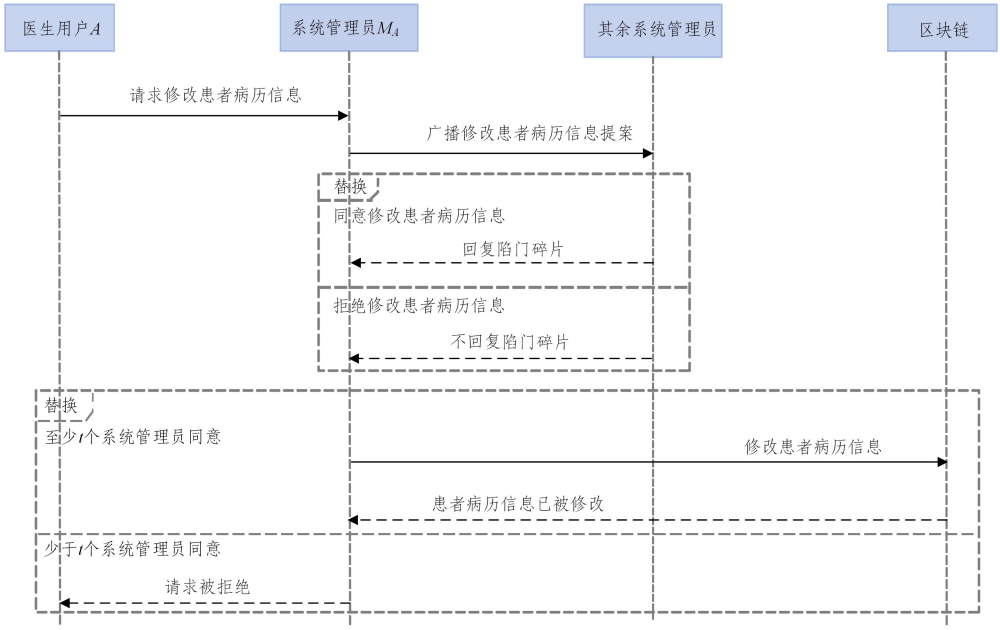

图 2 数据管理流程时序图

Fig. 2 Sequence diagram of data management process

3.2.4 区块链结构设计

本文提出的医疗联盟链结构如图 3 所示。其中，主链存储患者的医疗数据密文，而侧链存储主链发生修改的相关修改证明，包括用于查找修改证明的索引、该病人电子病历原始

消息的哈希值、修改后的新消息的哈希值、修改人身份标识与修改时间，具体结构如图 4 所示。

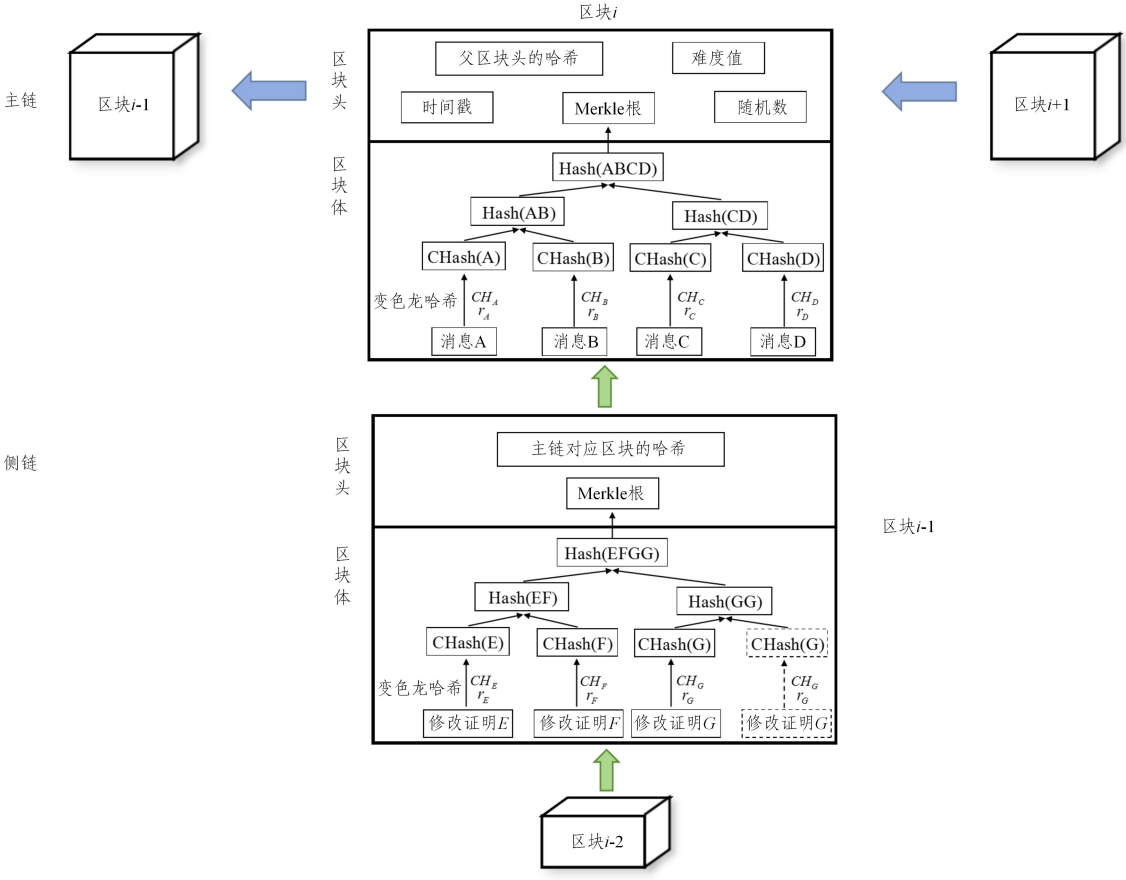

图 3 “主-侧”链结构示意图

Fig. 3 Structure diagram of “main-side” chain

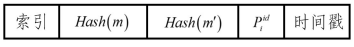

图 4 修改证明结构图

Fig. 4 Structure of modification certificate

假设区块链主链中第 i 个区块中的消息 m_B 需要修改，该信息对应的原始变色龙哈希值为 $CHash(B)$，则先将消息 m_B 的具体内容更新为 m_B'；再利用 Forge 算法生成与新消息对应的新可变参数 r'，使 r' 与 $CHash(B)$，m_B' 相匹配。若在给定时间 Δt 内存在多条信息发生修改，则由这段时间内最后一位进行信息修改的系统管理员对这些消息进行分类，选择属于某病人的电子病历信息修改证明，将它们打包在一个区块中，再将其连接到该病人主链对应区块的侧链上。基于该模型，医生用户与系统管理员均不需要下载完整区块链，有效节约了存储空间。当需要进行数据审查或追溯相关修改证明时，管理员通过请求邻居节点下载相关的侧链区块，依据区块中修改证明的索引即可按序追溯修改的历史记录，其中 P_A^{id} 标记修改者的身份，原始消息与新消息的哈希值表明修改者是否正确完成修改操作。

4 安全性分析

1)陷门的安全性

在本文提出的医疗数据管理方案中，系统完整公钥 $PKey$ 是由各医疗机构的系统管理员共同生成的公共参数，由前文可知，系统完整公钥 $PKey$ 的计算式为：

$$PKey=g^{\sum_{i=1}^{n}x_i}=g^{T}(\mathrm{mod}\ p)$$

若已知变色龙哈希函数陷门 T，则很容易计算出系统公钥 $PKey$。反之，若仅仅知道公钥 $PKey$，想要计算出系统的完整陷门 $T=\log_g PKey(\mathrm{mod}\ q)$，为离散对数问题[15]，而有限域上的离散对数问题是困难问题。因此，在仅知道完整公钥 $PKey$ 的情况下是无法计算出变色龙哈希函数的完整陷门 T 的。

2)秘密共享的安全性

当提出修改申请的系统管理员调用 $ReTrapdoor$ 函数恢复系统完整陷门时，必须获取到超过阈值 t 个的陷门碎片 x_i 与对应的 $f(x_i)$，才能够构造出 t 阶线性方程组，求解出唯一正确的 a_i 与 s，构造出的 t 阶线性方程组如下所示：

$$\begin{cases} f(x_1)=s+a_1x_1+a_2x_1+\cdots+a_{t-1}x_1^{t-1} \\ f(x_2)=s+a_1x_2+a_2x_2+\cdots+a_{t-1}x_2^{t-1} \\ \cdots \\ f(x_t)=s+a_1x_t+a_2x_t+\cdots+a_{t-1}x_t^{t-1} \end{cases}$$

显然，若无法获取到大于等于 t 个 $(x_i,f(x_i))$，则无法求解出该 t 阶线性方程组，这表明构造出的 t 阶线性方程组有效保证了秘密共享的安全性。

3)变色龙哈希函数的安全性

假设有一外来恶意攻击者，想要在仅知道系统公共参数 $\{p,q,g,PKey\}$ 的情况下，将区块链上原始消息 m 篡改为新消息 m'，则其需要令篡改前后变色龙哈希值保持不变，即令：

$$CH(m,r)=CH(m',r')$$

$$g^{m}PKey^{r}=g^{m'}PKey^{r'}(\mathrm{mod}\ p)$$

$$g^{m+T\cdot r}=g^{m'+T\cdot r'}$$

由于该外来攻击者无法获取系统完整陷门 T，则其无法计算出新消息 m' 对应的新随机数 r'，也就无法篡改链上原始消息，系统安全性未被破坏。

假设在所有医疗机构的 n 位系统管理员中，有 $i(i\in[1,t))$ 位系统管理员变为恶意节点，他们想要联合篡改区块链上的原始消息 m。在他们已知系统公共参数 $\{p,q,g,PKey\}$ 和其分别持有的陷门 $\{x_1,x_2,\cdots,x_i\}$ 的情况下，需要计算出新随机数 r' 来保证篡改前后变色龙哈希值与原来保持一致，原始的变色龙哈希值为：

$$\begin{aligned}CH(m,r)&=g^m PKey^r \pmod p\\&=g^m\left(\prod_{i=0}^{n}y_i\right)^r \pmod p\\&=g^m\left(g^{x_1}g^{x_2}\cdots g^{x_i}\cdot y_{i+1}y_{i+2}\cdots y_n\right)^r \pmod p\\&=g^{m+x_1+x_2+\cdots+x_i}\cdot\left(y_{i+1}y_{i+2}\cdots y_n\right)^r \pmod p\end{aligned}$$

而篡改后的变色龙哈希值表达式为：

$$CH(m',r')=g^{m'+x_1+x_2+\cdots+x_i}\cdot\left(y_{i+1}y_{i+2}\cdots y_n\right)^{r'} \pmod p$$

由上式可知，联合的恶意节点无法获得剩余公钥碎片关于 g 的关系式，进而无法计算出新消息对应的随机数 r'，因此无法篡改链上消息。

综合上述两种情况分析，无论是外来恶意攻击者，还是区块链系统中联合起来的恶意节点，均无法在未知变色龙哈希函数完整陷门的情况下篡改链上消息，表明了该方案的安全性。

4）区块链结构设计的安全性

本文设计的方案中，主链区块用于存储患者的医疗数据，对应的侧链区块存储属于患者的医疗数据的修改证明。这样的设计保证了管理员对于医疗数据编辑的透明性，使得所有的数据编辑行为是可追溯的，为数据审查提供了依据，避免了攻击者恶意篡改主链数据而不被发现，提升了整个区块链系统的安全性。假设某侧链区块内部的 Merkle 树如图 5 所示。

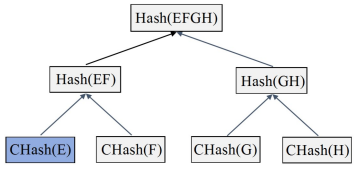

图 5 侧链区块 Merkle 树示意图

Fig. 5 Diagram of sidechain block Merkle tree

如图 5 所示，假设存在恶意节点质疑某合法的管理员节点 M_A 是否正确完成消息 m_E 的修改操作，一方面，该管理员节点 M_A 可以通过请求保存有消息 m_E 的修改证明 E 的节点提供 SPV 证明[16-17]($CHash(F)$，$Hash(GH)$)来证明修改操作已被记录在链；另一方面，M_A 可以直接请求保存修改证明 E 的侧链区块，通过索引快速查询到修改证明 E，依据身份标识 P_A^{id}，消息 m_E 及修改后的消息 m_E' 的哈希值自证清白。因此，本文提出的主-侧结构的区块链是安全的。

5 性能分析

5.1 实验环境

为了能够很好的评估所提出的医疗数据管理方案的效率，本文通过实验给出各阶段的算法运行时间。该实验主要由 Java 语言编写，实验具体环境配置如表 2 所列。

表 2 实验环境配置信息

Table 2 Experimental environment configuration information

实验环境	型号/版本
编程语言	JDK1.8
编译器	IntelliJ IDEA 2023.1.1
主机配置	Intel(R) Core(TM) i9-12900CPU

5.2 基本算法执行速率

设置安全参数 λ 的值为 256，且有 p,q,g 满足 $p=kq+1$，$g^q\equiv1 \pmod p$。执行 100 次系统参数生成算法，取平均值后可得其执行一次的速率约为 193 ms。本文所提方案仅涉及模加、模乘、幂模和哈希这 4 种基本运算，因此选定长度为 256 位随机数，执行各运算 500 次后的平均时间来代替其执行一次的速率，从而得到更为准确合理的结果（见表 3）。

表 3 基本运算执行速率

Table 3 Basic operation execution rate

符号	说明	时间/ms
T_a	进行 500 次模 p 加法运算的平均时间	0.027
T_m	进行 500 次模 p 乘法运算的平均时间	0.230
T_g	进行 500 次幂模 p 运算的平均时间	53.840
T_h	进行 500 次 SHA-256 运算的平均时间	0.015

5.3 各阶段执行速率

本文所提医疗数据管理方案包含 3 个阶段：区块链初始化、主链区块生成和医疗数据修改与验证阶段，涉及系统安全参数生成算法 SetUp、系统完整陷门生成算法 TrapdoorGen、系统完整公钥生成算法 PKeyGen、变色龙哈希值算法 Chash、消息签名算法 Signature、完整陷门重构算法 ReTrapdoor、新随机数生成算法 Forge 和验证算法 Verify。依据基本算法的执行速率，结合系统管理员人数 n 与系统门限值 t，可得各阶段的理论执行时间，如表 4 所列。

表 4 各阶段执行时间

Table 4 Execution time of each phase

阶段	算法	执行时间表达式/定值
区块链初始化	SetUp	193ms
	TrapdoorGen	$(nt-1)T_a+\frac{nt(t-1)}{2}T_m$
	PKeyGen	$nT_g+(n-1)T_m$
主链区块生成	Chash	$2T_g+T_m$
医疗数据修改	Signature	签名：$t(T_h+T_g+T_m)$ 验证：$t(T_h+2T_g+T_m)$
	ReTrapdoor	—
	Forge	T_m+2T_a
医疗数据验证	Verify	$2T_g+T_m$

由于 ReTrapdoor 算法需要求解 t 阶线性方程组，其运行时间与门限值和总人数直接相关，故表 4 未给出具体执行速率表达式。此外，同意修改数据的系统管理员与指定的系统管理员进行消息传递的过程中，根据 Signature 算法进行消息的签名与验证的总时间取决于门限值 t 的取值，另外还涉及消息接收的时延，且有可能出现消息验证失败后的超时重发。因此，本文对医疗数据修改阶段进行进一步的实际模拟，以探究该阶段更为准确的执行速率。

当想要恢复系统完整陷门 T 时，系统管理员需要先接收其他同意修改的管理员发送的陷门碎片信息，即该阶段的执行速率包含该管理员使用 Signature 算法进行验证的时间。收集到阈值 t 的正确陷门碎片后，调用 ReTrapdoor 算法恢复

T，然后执行 Forge 算法计算出新的随机数，最终完成医疗数据的修改。由表 4 可知上述过程的总时间 T_t 是关于阈值 t 的函数，因此能够绘制出当阈值 t 变化时，医疗数据修改阶段需要的总时间，如图 6 所示。

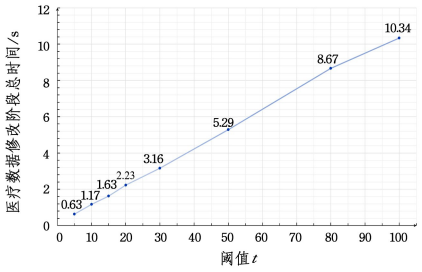

图 6　医疗数据修改阶段总时间

Fig. 6　Total time of medical data modification phase

接下来，基于上述系统参数，设置阈值 $t=15$，权限节点数 $n=20$，将本文方案在数据修改阶段的时间开销与文献[9]和文献[18]相比较，其数值结果如图 7 所示。具体而言，在本文方案中，试图恢复完整陷门的系统管理员在收到其余管理员传递的陷门碎片后，需要利用 Signature 算法来验证陷门碎片是否来自于对应的管理员，且需要保证该信息未被篡改，否则需要等待超时重传信息。这样能够有效保证陷门恢复与数据修改的正确性，但也增加了一定的时间开销。在文献[18]中，负责修改数据的管理员不必恢复完整陷门，而是通过收集各节点分享的随机数份额来直接生成新的随机数，以完成对数据的修改。但是这一过程的时间开销变动较大。最优情况下，即所有节点同时计算随机数份额并发送，数据修改阶段执行时间的表达式为 $3T_g+(t+1)T_m$，花费的时间为 233ms。而最差情况下，即所有节点依次完成计算，这样数据修改阶段执行时间的表达式为 $t(3T_g+2T_m)+(t-1)T_m$，需要 2 538 ms。然而，最优情况作为理想假设是难以实现的，大部分情况下所花费的时间较长且并不稳定。而本文方案对于某条数据修改的时间则趋于常数，且在文献[18]的范围内。此外，本文方案并不涉及投票选择修改人，而是由发出提案的管理员进行实际编辑操作，相较于文献[18]平均节省 53 ms。文献[9]的方案与本文类似，都需要利用完整陷门生成新的随机数，但不涉及信息验证和秘密分享过程，其在该阶段执行时间的表达式为 $T_m+(t+2)T_a$，在大幅减少时间开销的同时却也严重降低了安全性，如可能导致变色龙哈希验证失败。综上所述，本文方案在医疗数据修改阶段产生的计算开销是可以接受的，且整体具有良好的执行效率。

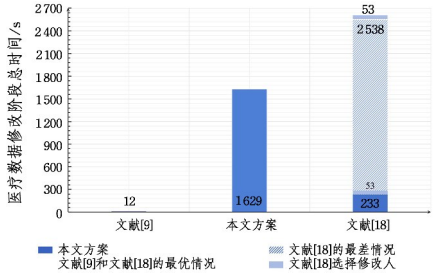

图 7　医疗数据修改阶段计算开销对比

Fig. 7　Comparison of computation time during medical data modification phase

此外，对于区块链初始化阶段，本文方案与文献[9]类似，但相较于文献[18]更为简洁。本文方案仅需生成系统公共参数、变色龙哈希公私钥对并分发陷门碎片，而文献[18]在此基础上还需要为每个节点生成用于数字签名的公私钥对和对陷门碎片进行再分享，在一定程度上增加了时间开销。同样地，在区块验证阶段，本文提出的方案不需要像文献[18]中引入监管者来专门验证修改前后的哈希值和编辑者身份，只需要各位管理员自行验证并更新本地数据库中的信息，有效减少了验证的时间开销，提高了数据修改的效率。

5.4　医疗数据修改阶段通信开销分析

医疗数据修改阶段是数据管理方案的核心部分，因此选择该阶段将本文方案与文献[9]、文献[18]进行通信开销的对比[19]分析。

在该阶段，为恢复系统完整陷门，所对比的方案均是由持有系统私钥的系统管理员向负责进行修改的管理员传递信息。本文方案所传递的信息为陷门碎片 x_i、有限域 Z_q^* 上的多项式 $f(x_i)$和签名 sig，文献[9]仅传递管理员子私钥 s_i，而文献[18]向各节点发送随机数份额，如图 8 所示。

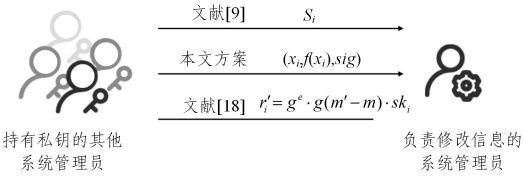

图 8　医疗数据修改阶段信息传递示意图

Fig. 8　Diagram of information transmission during medical data modification phase

在安全参数 λ 的值为 256 的条件下，文献[9]中的每位系统管理员传递的子私钥大小即为 256 bit。对于本文方案，陷门碎片 x_i 与多项式 $f(x_i)$均为 256bit，而签名 $sig=(h,s,y_i)$ 大小为 768 bit，即每位系统管理员传递 1 280 bit 大小的信息。文献[18]的每位管理员需要传递的随机数份额分享的大小也为 256 bit。虽然本文在医疗数据修改阶段的通信开销略大于文献[9]与文献[18]，但并没有直接传输系统陷门碎片或随机数，提高了传输过程的安全性。与此同时，在本文方案中，消息发出方需要对陷门碎片进行签名，以确保接收方收到正确的碎片信息，签名 sig 信息牺牲了较大的通信开销，但保证了信息未被恶意篡改。因此，本文的通信开销是合理的且可以被接受的。

5.5　侧链区块存储空间

在本文所设计的区块链结构中，每个主链区块存储某位患者的医疗数据，该区块对应的侧链则存储主链区块的数据修改证明。然而，并不是每个用户节点都需要下载完整区块链，只需要在需要追溯相关修改证明或进行审查时下载相关侧链，从而节约了存储空间。

侧链区块由区块头和区块体构成，区块头中存储主链对应区块哈希值和该区块中的 Merkle 根，大小均为 32 字节，而区块体中存储数条修改证明。假设一条修改证明的长度为 $|MX|$字节，且一个区块中平均存储 a 条修改证明，则一个侧链区块的大小为 $64+a|MX|$字节。因此，如果完整区块链中共存在 b 个侧链区块，在正常使用电子病历存储病人信息的情况下，能够节省 $b(64+a|MX|)$字节的存储空间。相较于因记录历史修改数据而增大原区块链主链大小的方案[20-21]，本文方案恰好节约了这些存储空间。

结束语 本文提出了一种面向联盟链的安全、可追责的医疗数据管理方案，各医疗机构预选出的系统管理员分别持有变色龙哈希函数的陷门碎片，参与生成系统公钥并在医疗数据修改阶段恢复完整陷门。设计了“主-侧”链结构的可编辑区块链模型，实现对数据修改的可靠追责，而可验证的签名方案则保证了医疗数据修改的正确性，有效解决了面向医疗联盟链的数据管理方案存在的问题。安全性分析和相关的实验结果表明，本文方案具有良好的安全性，且各阶段运行效率良好。考虑到本文方案并未对预选出的管理员进行管理，下一步的工作则需要增加系统管理员入职、离职等基本管理机制。

参 考 文 献

[1] NIE F B. Research on Blockchain-based Medical Data Management Methods [D]. Changsha: Central South University, 2024.

[2] YE T, LUO M, YANG Y, et al. A survey on redactable blockchain: challenges and opportunities [J]. IEEE Transactions on Network Science and Engineering, 2023, 10(3): 1669-1683.

[3] ATENIESE G, MAGRI B, VENTURI D, et al. Redactable blockchain-or-rewriting history in bitcoin and friends[C]// 2017 IEEE European Symposium on Security Pnd privacy (EuroS&P). IEEE, 2017: 111-126.

[4] YUAN Y, WANG F Y. Editable Blockchain: Models, Techniques and Methods[J]. Journal of Automation, 2020, 46(5): 831-846.

[5] AZARIA, EKBLAW A, VIEIRA T, et al. MedRec: Using Blockchain for Medical Data Access and Permission Management [C]// 2016 2nd International Conference on Open and Big Data (OBD). Vienna, Austria, 2016: 25-30.

[6] XUE T F, FU Q C, WANG C, et al. A Medical Data Sharing Model via Blockchain[J]. Journal of Automation, 2017, 43(9): 1555-1562.

[7] ZHANG C, LI Q, CHEN Z H, et al. Medical Chain: Alliance Medical Blockchain System [J]. Journal of Automation, 2019, 45(8): 1495-1510

[8] ZHAO X Q, ZHANG Z H, LI Y. An Editable and Accountable Blockchain Scheme[J]. Journal of Information Security, 2022, 7(5): 19-28.

[9] LV W L, WEI S J, YU M H, et al. Research on Verifiable Blockchain Ledger Redaction Method for Trusted Consortium [J]. Journal of Computers, 2021, 44(10): 2016-2032.

[10] WANG X, ZHENG D, GUO R. Electronic Medical Record Sharing Solution for Editable Blockchain [C]// 2021 3rd International Conference on Natural Language Processing (ICNLP). Beijing, China, 2021: 93-103.

[11] MARSALEK, ZEFFERER T. A Correctable Public Blockchain [C]// 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE). Rotorua, New Zealand, 2019: 554-561.

[12] JIA M, CHEN J, HE K, et al. Redactable Blockchain From Decentralized Chameleon Hash Functions[J]. IEEE Transactions on Information Forensics and Security, 2022, 17: 2771-2783.

[13] ZHANG C, NI Z, XU Y, et al. A trustworthy industrial data management scheme based on redactable blockchain[J]. Journal of Parallel and Distributed Computing, 2021, 152: 167-176.

[14] LI M, JIA C, DU R, et al. DSE-RB: A privacy-preserving dynamic searchable encryption framework on redactable blockchain [J]. IEEE Transactions on Cloud Computing, 2023, 11(3): 2856-2872.

[15] BERA B, CHATTARAJ D, DAS A K. Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment[J]. Computer Communications, 2020, 153: 229-249.

[16] SHI J, ZHANG A, BAI X Y, et al. Survey on Performance Optimization Technologies of Distributed Ledger System[J]. Journal of Software, 2023, 34(10): 4607-4635.

[17] LI G Z, LI L X, GAO H Y. Cross-Chain Technology Development and Application Research [J]. Computer Engineering and Applications, 2024, 60(2): 32-45.

[18] LAI M X, DU R Y, CHEN J, et al. A Decentralized and Accountable Redactable Blockchain Scheme [J/OL]. Journal of Wuhan University (Science Edition). [2024-03-05]. https://kns.cnki.net/kcms2/detail/42.1674.N.20230626.1009.004.html.

[19] CHEN Y B, ZHONG C R, ZHOU C R, et al. Design of Cross-domain Authentication Scheme Based on Medical Consortium Chain[J]. Computer Science, 2022, 49(S1): 537-543.

[20] JIA Y, SUN S F, ZHANG Y, et al. Redactable Blockchain Supporting Supervision and Self-Management[C]// ASIA CCS '21: ACM Asia Conference on Computer and Communications Security. ACM, 2021.

[21] MATZUTT R, AHLRICHS V, PENNEKAMP J, et al. A moderation framework for the swift and transparent removal of illicit blockchain content [C]// 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2022: 1-9.

TAN Jingqi, born in 2003, undergraduate. Her main research interests include information security and blockchain.

HUANG Haiping, born in 1981, Ph.D, professor, Ph.D supervisor, is a member of CCF(No. 15253S). His main research interests include information security and data privacy in IoT.