基于Hyperledger Fabric的电子病历共享方案

陈嘉莉[1,2]，马自强[1,2]，苗莉[1,2]，李冰雨[3]，岳晓琳[1,2]
（1. 宁夏大学信息工程学院，宁夏 银川 750021；2. 宁夏大数据与人工智能省部共建协同创新中心，宁夏 银川 750000；
3. 北京航空航天大学网络空间安全学院，北京 100083）

摘　要：针对电子病历的存储安全与共享过程中涉及的病历所有权及访问控制问题，提出了一种基于Hyperledger Fabric的电子病历共享解决方案。在此方案中，电子病历通过智能合约实现的代理重加密技术，根据是否需要共享的条件，被加密并存储在星际文件系统（IPFS）中。病历的IPFS地址将被记录在区块链上，以确保其不可篡改性。在共享病历时，患者将制定严格的访问控制策略，借助基于属性的加密（CP-ABE）和Asmuth-Bloom秘密共享算法，确保电子病历仅能被经过授权的人员访问。同时，参与秘密分发的各方将协作恢复密钥，进而解密病历。所提方案在安全性方面进行了全面阐述，确保电子病历在存储与共享过程中能够抵御各类攻击，保证数据的完整性和隐私性。与其他秘密共享方案相比，所提方案在理论上的时间复杂度上表现出色，为电子病历的安全存储与多人共享提供了高效且可靠的解决方案。

关键词：Hyperledger Fabric；电子病历共享；代理重加密；Asmuth-Bloom秘密共享算法
中图分类号：TN309
文献标志码：A
DOI：10.11959/j.issn.1000−436x.2024218

Electronic medical records sharing solution based on Hyperledger Fabric

CHEN Jiali[1,2], MA Ziqiang[1,2], MIAO Li[1,2], LI Bingyu[3], YUE Xiaolin[1,2]
1. School of Information Engineering, Ningxia University, Yinchuan 750021, China
2. Ningxia Big Data and Artificial Intelligence Collaborative Innovation Center, Yinchuan 750000, China
3. School of Cyberspace Security, Beihang University, Beijing 100083, China

Abstract: In addressing the issues of medical record ownership and access control during the storage and sharing processes of electronic medical record (EMR), an EMR sharing solution based on Hyperledger Fabric was put forward . In this solution, EMR was encrypted and stored in IPFS (inter planetary file system) using proxy re-encryption technology implemented through smart contracts, depending on the conditions for sharing. The IPFS addresses of the records were recorded on the blockchain to ensure their immutability. For sharing EMR, patients established strict access control policies. Through the use of CP-ABE (attribute-based encryption) and the Asmuth-Bloom secret sharing algorithm, the EMR was encrypted so that only authorized personnel can access them. Simultaneously, parties involved in secret sharing collaborate to recover keys and decrypt the records.The document comprehensively discusses the security aspects of this solution, ensuring that EMR can withstand various attacks during storage and sharing, thus guaranteeing data integrity and privacy. Compared to other secret sharing schemes, this solution demonstrates better theoretical time complexity, providing an efficient and reliable solution for secure storage and multi-party sharing of EMR.

Keywords: Hyperledger Fabric, electronic medical records sharing, proxy re-encryption, Asmuth-Bloom secret sharing algorithm

---

收稿日期：2024−10−10
通信作者：马自强，maziqiang@nxu.edu.cn
基金项目：宁夏回族自治区重点研发计划一般基金资助项目（No.2022BDE03008）
Foundation Item： General Project of Key Research and Development Program of Ningxia Hui Autonomous Region (No.2022BDE03008)

0　引言

在现代医疗信息技术迅速发展的时代，电子病历作为医疗信息化的核心组成部分，已成为医疗领域中不可或缺的重要信息资产。尽管电子病历的地位重要，但其管理和共享仍面临多重挑战[1]。病历数据容易被篡改或泄露，传输和存储过程中可能导致数据丢失或恶意篡改，从而难以确保数据的完整性和真实性。当前大多数医疗机构使用的电子病历系统多为封闭体系，缺乏有效的信息互通机制。患者在跨机构就诊时通常需要重复填写个人病历信息，浪费时间和精力，同时可能因信息传递不准确或不完整而影响诊疗效果[2]。

面对上述挑战，寻求既安全可靠、又透明高效的电子病历共享解决方案显得尤为迫切。在此背景下，基于区块链技术的电子病历共享方案脱颖而出，为医疗信息管理开辟了全新的可能性。首先，区块链技术的去中心化特性与强大的加密机制，能够防止病历数据遭到篡改或非法盗用。其核心原理在于，每一个数据块均包含前一数据块的哈希值[3]，由此形成一条坚不可摧的链式结构，确保了数据的安全性。此外，区块链采用分布式存储方式，将数据分散保存在众多节点上，增强了数据防护能力，降低了单一节点故障或攻击对整体数据安全的影响。最重要的，区块链具有“一旦写入，不可更改”的特性，所有对数据的操作行为都将被忠实记录于区块链上，形成公开透明、可追溯的交易历史。这一特性确保了病历数据的完整性和真实性，使得医疗机构与患者都能便捷地验证数据真伪，为构建高效、安全、互信的医疗信息生态环境奠定了坚实基础。

随着基于区块链的电子病历共享方案的发展，尽管解决了许多传统系统的问题，但仍面临一些挑战。首先，在安全存储方面，尽管区块链能保障数据安全，但将病历数据完全存储在链上会降低效率，因此通常采用链上链下结合的方式，需对链下数据进行加密。其次，病历共享时需解密获取明文病历，密钥管理在保障数据机密性上至关重要，有效的密钥管理机制需进一步完善，以确保密钥安全交换，防止泄露或滥用。此外，针对多机构共享的访问控制，需要建立灵活精细的权限机制，以适应不同机构的数据访问需求，确保只有授权用户能访问特定病历，保护患者隐私。并且，尽管区块链能实现患者对病历信息的授权管理，但如何方便患者控制数据访问权限，同时平衡患者的控制权和医疗机构的合法需求，仍需深入研究和完善。综上所述，目前电子病历共享仍存在以下问题。

1) 隐私保护难题：在电子病历共享过程中，需要确保患者的个人隐私不被泄露，避免数据在传输、存储和访问过程中被非法获取或篡改。

2) 数据共享安全挑战：不同医疗机构之间的系统可能采用不同的安全标准和防护措施，这增加了数据共享过程中的安全风险。同时，网络攻击、系统漏洞等外部威胁也可能对数据共享过程造成破坏。

3) 权限控制复杂性：在推动分级诊疗的过程中，需要合理设置不同医疗机构和医护人员访问电子病历的权限。权限设置不当可能导致信息泄露，也可能阻碍医疗资源的有效配置和患者的及时救治。

基于此，本文提出一个基于区块链的电子病历共享方案，主要研究工作如下。

首先，根据是否共享决定数据加密方式，确保机密性，允许共享的电子病历可由患者和医生分别使用各自私钥解密，提高密钥安全性。具体为，对电子病历区分是否共享进行分别加密。不允许共享的病历采用患者的公钥加密存储，允许共享的病历需要再次加密处理，采用患者的公钥加密后，再通过获取的重加密密钥对首次加密的密文进行再次加密，使得诊断医生能够用自己的私钥解密病历信息。

其次，在分级诊疗体系下，结合基于密文策略的属性基加密（CP-ABE）和Asmuth-Bloom秘密共享算法，实现了更为精细和安全的病历访问控制。患者制定访问控制策略管理病历，医生根据策略获取子密钥解密电子病历，实现多机构安全共享。患者制定的访问控制策略管理病历访问树结构并使用Asmuth-Bloom算法分发其私钥作为子密钥，与访问控制策略的叶子节点对应。医生根据策略请求数据以获取子密钥，从而重构解密电子病历的密钥，实现多机构间安全共享。

最后，在Hyperledger Fabric平台上实现了电子病历共享方案。在方案中，利用智能合约将代理重加密算法的逻辑嵌入智能合约中，实现了自动化密

钥分发过程。电子病历根据是否需要共享的条件，通过智能合约进行加密并存储在星际文件系统（IPFS）中，其IPFS地址记录在区块链上，确保数据的不可篡改性。实验结果表明，该方案在实际应用中表现良好，能够有效地保障电子病历的安全存储与高效共享。

1 相关工作

不同研究者提出了多种基于区块链的医疗数据共享方案，旨在解决电子病历数据安全问题和共享问题。薛腾飞等[4]提出了基于区块链的医疗数据共享模型，初次利用区块链的去中心化和安全可信特性，解决了医疗机构间数据共享的难题，采用了多种加密和共识机制以确保数据安全性和共享效率。然而功能单一，安全性较弱。周辉等[5]提出基于区块链的数据共享模型和数据访问权限控制模型，解决了电子医疗数据共享的问题，但是该模型没有具体考虑到存储和共享的安全问题。徐健等[6]提出基于区块链的医疗记录安全存储与访问方案，重视非对称加密的密钥管理和安全分发。然而，在数据共享过程中，存在密钥传播可能导致的泄露风险，需要进一步加强用户隐私信息的安全性。朱诗生等[7]结合非对称和对称加密算法，设计医疗数据安全共享模型，关注密钥生成和安全传输问题。但无论是单一的加密方式还是混合的加密后存储的方案，都有密钥管理的问题，并且在交换密钥过程中不安全。罗文俊等[8]提出的基于区块链的电子医疗病历共享方案是对Cui等[9]的改进，设计了数据安全共享协议，将分布式密钥生成技术和基于身份的代理重加密方案相结合，以提高密钥管理的安全性。

针对病历共享的问题，郭庆等[10]提出支持受控共享的医疗数据隐私保护方案，将区块链与代理服务器结合设计医疗数据受控共享模型，区块链矿工节点分布式构造代理重加密密钥，使用代理服务器存储和转换医疗数据密文，利用代理重加密技术在保护患者隐私的同时实现医疗数据共享，然而引入第三方存在信息泄露的风险。唐飞等[11]提出了基于区块链和条件代理重加密的电子处方共享方案。其中的条件代理重加密方案提供了一种密文的高效转发机制，并实现了解密权限的细粒度划分。该方案利用分布式密钥生成技术解决了密钥托管问题，适用于复杂的区块链应用场景，能够在改善密钥泄露的同时实现数据共享。庞震等[12]提出了基于云存储、区块链和智能合约的安全共享机制，实现了医疗数据在医院间和医院与科研机构间的快速、安全共享。

针对电子病历共享过程中多机构的访问控制问题，Thwin等[13]将Ateniese提出的加密方案与区块链技术相结合，构建用户医疗数据访问控制策略方案。李腾等[14]设计了一种多客户端的医疗信息共享方案，将多个医院组成联盟链，用于存储电子健康记录索引，并使用了拜占庭共识算法来增加索引的可靠性。该方案结合可搜索加密和属性加密技术，实现了细粒度的访问控制，保护了信息安全，但数据动态处理和修改删除功能仍需改进。此外，由于电子病历系统缺乏统一标准，跨院数据共享困难重重。金琳等[15]提出了一种基于多权限的属性隐藏加密算法，该算法可以在隐藏策略下实现可追溯性，支持灵活的访问结构，并且能够部分隐藏属性，以保护用户隐私。结合线性秘密共享方案，该算法将属性分为两部分，从而保护了属性的隐私并实现了跨机构的多人共享。闫冠辰等[16]提出了一套跨院的电子病历共享系统，该系统统一了电子病历数据格式，并利用区块链平台进行数据存储。使用高效的SHVE算法实现了医生跨科室查询患者诊疗信息的功能，同时对敏感数据使用CP-ABE算法。该系统具备数据加解密、安全检索等功能，包括模糊查询。孙晓晔等[17]提出基于联盟链的面相研究机构的医疗信息共享平台，采用了“区块链+云服务器”的存储方式。病案数据以密文形式存储和传输，该模型采用基于属性的访问控制（ABAC, attribute-based access control）实现对病案细粒度访问，最大程度保护了患者隐私。智能合约用于保证交易的可靠性和高效性。然而，该研究未考虑病历归属权以及患者对个人医疗信息的处理同意权。

综上所述，研究者们提出了多种基于区块链的电子病历共享方案，这些方案利用了包括智能合约、代理重加密和多权限属性隐藏在内的多种技术手段，以确保医疗数据的存储、传输和访问安全，并提高了数据共享的效率和安全性。尽管这些方案在数据保护方面取得了一定的成效，但仍存在例如，密钥管理存在的安全漏洞、医疗数据访问授权

机制的不完善以及跨院数据共享的灵活性差等问题。本文将提出基于Hyperledger Fabric的电子病历共享方案，以解决目前存在的不足，提高电子病历共享系统的安全性和隐私性。

2　预备知识

2.1　代理重加密

代理重加密[18]是基于公钥加密方案的一种。在代理重加密方案中，使用了公钥加密算法来实现消息的加密和解密操作。代理重加密方案被Blaze等[18]首次提出，该方案是通过委托人生成代理重新加密密钥并发送给代理服务器，代理服务器能够将使用委托人的公钥加密的数据转化为使用另一委托方的公钥加密的数据。此过程无需使用委托人的私钥解密数据，能实现密文的安全共享，还保护了各个委托方的隐私安全，详细过程如下。

1) 用户A用自己的公钥PK_A加密明文M，得到密文C_A，$C_A = E_A(\mathrm{PK}_A, M)$。

2) A生成用于B的代理重加密密钥$\mathrm{RK}_{A\to B}$，并将密文C_A和$\mathrm{RK}_{A\to B}$发给代理。

3) 代理利用$\mathrm{RK}_{A\to B}$将密文C_A转换为C_B，代理只进行密文转换，不知道明文内容。

4) 代理将C_B发送给B，B使用自己的私钥解密便可获得明文。

2.2　困难问题模型

DBDH问题是在双线性对上的一个离散对数问题，用于构建一些特定类型的密码体制。其中离散对数问题（DLP）和计算Diffie-Hellman问题（CDH）是在密码学中经常用到的2个基本问题。

1)DLP：已知G_1中的两点A和B，且$A = B^n$，很难找到$n \in Z_p^*$使得$A = B^n$。

2)CDH[19]：已知G_1中的点A，对于给定的(A, A^m, A^n)，很难计算A^{mn}中的$m, n \in Z_q^*$。

2.3　属性基加密

属性基加密通常指的是基于属性的加密（ABE）[20]，允许用户使用一系列属性来加密和解密数据，而不局限于传统的基于身份的加密。在属性基加密中，数据的解密取决于用户的属性，而不是特定的密钥或身份。这使得属性基加密在访问控制和数据共享方面非常有用，该方案可以确保只有拥有特定属性的用户才能解密和访问数据。属性基加密目前已经在许多领域得到应用，包括医疗保健、云计算、物联网和多方安全计算等，为数据安全和隐私提供了更灵活的控制方式，使得数据所有者能够更精细地管理数据的访问权限[21]。

基于属性的加密通常分为2种，基于密钥策略的属性加密（KP-ABE）和基于密文策略的属性加密（CP-ABE）。基于密文策略的属性加密中加密过程的访问控制是基于密文的属性进行定义的。这种加密方法允许发送者对密文设置访问策略，要求解密者的密钥必须满足这些策略才能解密密文。在CP-ABE中，密文包含了数据和访问策略，而密钥则包含了用户的属性信息。解密者只有在其密钥的属性与密文的策略相匹配时才能成功解密密文，否则将无法获取明文信息。这种方式使得数据所有者可以以灵活的方式定义数据的访问权限，根据数据的属性或者接收者的属性来控制数据的访问。

2.4　Asmuth-Bloom秘密共享方案

Asmuth-Bloom秘密共享算法是一种秘密共享方案，由Asmuth和Bloom提出[22]。它是一种基于中国剩余定理的算法，该算法基于一个门限区间，这个门限区间从最大的$t-1$个互素整数是乘积到最小的t个互素整数的乘积，以下为该方案的具体内容。

1) 公开参数选择：选择一个互素的整数序列$(P_0, P_1, \cdots, P_n)$，其中，并且$P_0 \times P_{n-t+2} \times \cdots \times P_n < P_1 \times \cdots \times P_t$，$P_i$是与每个秘密分享者$U_i$相关的公开信息。$P_0 < P_1 < P_2 < \cdots < P_n$。

2) 秘密分发阶段：秘密s是一个随机整数且有$s \in Z_P^*$，秘密分发者任意选择正整数θ，计算$s = s + \theta P_0 \in \mathrm{GF}(P_{n-t+2} \times \cdots \times P_n, P_1 \times \cdots \times P_t)$，将秘密$s_i = s \bmod P_i (i = 1,2,3,\cdots,n)$分发给各个参与者。

3) 秘密重构阶段：给定一个m个参与者的集$(m \geqslant t)$利用参与者对应的秘密份额集合$\{s_{i_1}, s_{i_2}, \cdots, s_{i_m}\}$构造同余方程

$$\begin{cases} x = s_{i_1} \bmod P_{i_1} \\ x = s_{i_2} \bmod P_{i_2} \\ \vdots \\ x = s_{i_m} \bmod P_{i_m} \end{cases}$$

并通过中国剩余定理在Z_N上计算特殊解其中$N =$

$P_{i_1} \times P_{i_2} \times \cdots \times P_{i_m}$；$x = \sum_{j=l}^{m} \frac{N}{P_{i_l}} y_{i_l} s_{i_l} \bmod N$，由于$N > P_1 \times \cdots \times P_t$，因此该解为$Z_{P_1 \times \ldots \times P_t}$上的唯一解，则秘密恢复为$s = x \bmod P_0$。

2.5　Hyperledger Fabric

Hyperledger Fabric是一个由Linux基金会支持和维护的开源企业级区块链框架，专为满足复杂、多变的业务需求而设计。它采用了模块化的架构，提供了诸如智能合约（链码）、权限管理、隐私保护以及高效的共识机制等核心功能，为构建高度定制化、可扩展且安全的区块链应用提供了强大支持。

2.6　IPFS

IPFS作为一种创新的分布式文件系统，其核心优势在于其独特的存储与搜索机制。IPFS通过内容寻址（即基于文件内容的哈希值）来存储文件，每个文件或数据块都被赋予一个唯一的哈希标识符，这些标识符在全球范围内都是可访问的，从而实现了数据的去中心化存储与持久性。在搜索方面，IPFS利用分布式哈希表（DHT）技术，使得用户能够高效地根据文件的哈希值检索到所需的数据，无需依赖中心化的索引服务器。这种存储与搜索机制不仅提高了数据的安全性和可靠性，还极大地降低了数据冗余和传输成本，为构建更加高效、安全、去中心化的网络应用提供了坚实的基础。

3　系统模型

3.1　整体框架

本文方案主要由密钥生成中心（CA）、联盟链、患者、医生和IPFS存储机构5个实体组成。

1) CA：负责生成、管理、分发数字证书以及管理与证书相关联的密钥对。

2) 联盟链Hyperledger Fabric：以此为平台，用于支持智能合约的部署和执行，同时也可以代替第三方代理实现代理重加密方案中的自动密钥转换功能，存储IPFS的Hash值。

3) 患者：电子病历的所有者，管理自己的所有电子病历，运行智能合约，制定访问控制策略。

4) 医生：病历生成者，为患者诊断生成病历，并将自己的公钥一同发送给数据所有者，同时在其他转诊场景扮演数据请求者的角色或者恢复秘密的参与者。

5) IPFS：分布式存储机构，加密的电子病历存储在IPFS中返回地址Hash。

基于Hyperledger Fabric的电子病历共享方案的模型框架如图1所示，该模型分为2个子部分，分别是电子病历存储部分和电子病历共享部分。该模型整体流程为：1)区块链上的CA机构负责为患者和医生分发密钥，同时医生向区块链中的认证机构发送自己的属性，获取属性密钥；2)当患者在医院挂号后，接受对应医生的诊断，医生将附上自己的公钥，并将电子病历发送给患者；3)传入医生的公钥和患者的私钥通过智能合约，进行密钥转换，密钥转换完成后，患者将获得转换后的重加密密钥，并将对电子病历进行离线和在线加密，以便分别用于个人查看和共享；4)将其存储在IPFS中，IPFS会生成一个哈希地址存在链上；5)患者设定访问策略，并利用Asmuth-Bloom秘密共享算法，通过构造同余方程，将医生的私钥作为子秘密与同余方程中的参数一一对应，进行秘密分发；6)再就诊医生发出病历请求申请，请求访问电子病历；若通过患者设定的访问控制策略；7)获取存储在区块链上的IPFS哈希地址并获得密文；8)通过各个参与的秘密分享者合作，重构出解密电子病历的完整信息的密钥。这个过程使得数据请求者能够合法而安全地获取电子病历明文。

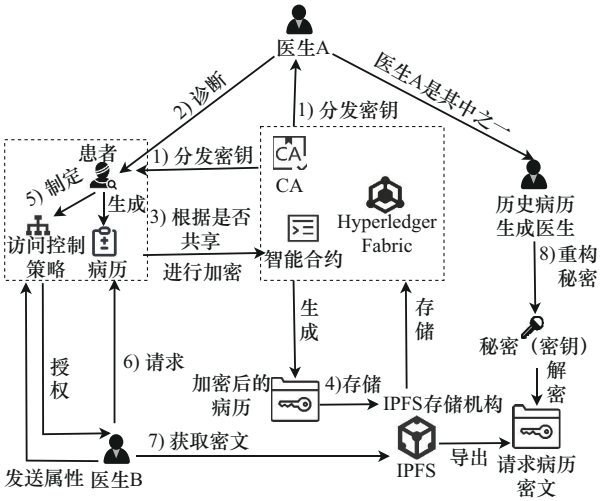

图1　基于Hyperledger Fabric的电子病历共享方案的模型框架

3.2　定义算法

本文模型由加密存储和共享两部分构成，加密存储部分由系统初始化、密钥生成、重加密密钥生成、电子病历离线加密、电子病历在线加密、解密

电子病历等算法构成，共享部分主要包括系统初始化、属性密钥生成、属性加密、秘密分发、秘密重构等算法构成，详细阐述如下。系统参数如表1所示。

表1　　系统参数

参数	含义
CA	证书颁发机构
Msk	主密钥
param	系统公共参数
Id	身份标识（P表示患者，D表示医生）
PK,SK	系统使用者的公钥和私钥
m	电子病历明文
m_{off}	离线加密电子病历密文
m_{on}	在线加密的电子病历明文
t	共享类型
RK	重加密密钥
m''	重加密密文
PK_S	共享阶段公共参数
MK_S	共享阶段主密钥
S	属性集合
SK_{Attr}	属性密钥
C	医生私钥（子秘密）
Γ	访问控制策略
C'	属性密文
I	秘密份额
K	秘密分享的分类门限序列
n	参与者个数
A	非授权子集
j	以科室种类分的类别

3.2.1　电子病历加密存储部分

1) $\text{setup}(1^k) \rightarrow (\text{param},\text{Msk})$：系统初始化，患者和医生通过Hyperledger Fabric中的CA认证，生成系统公共参数param和主密钥Msk。

2) $\text{Keygen}(\text{param},\text{Msk},\text{Id}) \rightarrow (\text{PK}_{\text{Id}},\text{SK}_{\text{Id}})$：密钥的生成由密钥生成中心完成，输入系统公共参数和主密钥，得到使用者的公钥和私钥，此处的使用者包括医生$(\text{PK}_D,\text{SK}_D)$和患者$(\text{PK}_P,\text{SK}_P)$。

3) $\text{KeyGen}_{\text{Re}}(\text{SK}_P,\text{PK}_D) \rightarrow \text{RK}_{P\rightarrow D}$：重加密密钥生成，输入系统参数、患者私钥和医生公钥，输出转换之后的重代理加密密钥$\text{RK}_{P\rightarrow D}$。

4) $\text{Encrypt}_{\text{off}}(\text{PK}_P,m,t) \rightarrow m'_{\text{off}}$：电子病历离线加密，患者对自己的病历使用个人公钥加密输出离线加密密文m'_{off}，在自己需要查看时能够方便查看。

5) $\text{Encrypt}_{\text{on}}(\text{PK}_P,\text{PK}_{P\rightarrow D},m,t) \rightarrow m'_{\text{on}}$：电子病历在线加密，患者就诊时使用公钥、是否允许共享类型t以及系统参数对电子病历加密得到在线加密密文m'_{on}。

6) $\text{ReEncrypt}_{\text{on}}(m'_{\text{on}},\text{PK}_{P\rightarrow D}) \rightarrow m''$：电子病历重加密，输入在线电子病历加密密文以及重加密密钥，最后输出重加密密文m''。

3.2.2　电子病历共享部分

1) $\text{Setup}(\lambda) \rightarrow (\text{PK}_S,\text{MK}_S)$：共享阶段初始化由联盟链上的可信机构CA执行，其功能是初始化系统以确保安全性。输入安全参数λ，该算法将安全参数转化为系统公共参数PK_S和系统主密钥MK_S。

2) $\text{AttrKeyGen}(\text{MK}_S,S) \rightarrow \text{SK}_{\text{Attr}}$：属性密钥生成算法由CA机构进行分发，输入包括公共参数PK_S和用户属性集合S，通过这些信息可以生成用户属性私钥SK_{Attr}。

3) $\text{AttrEncrypt}(C,S,\text{PK}_S,\Gamma) \rightarrow C'$：属性加密，输入待加密数据、参与方属性集合、公共参数和访问控制策略，最后输出为密文C'。

4) $\text{SecrShar}(C,(k,n),n,S) \rightarrow I_S(I_1,I_2,\cdots,I_n)$：输入秘密$C$，启用密钥解密所需的最低阈值，参与方也就是秘密共享者的个数n，输出属性值和对应的秘密份额I_S。

5) $\text{SecretRecov}(S_D,m) \rightarrow (\text{true},\text{false})$：数据共享及访问阶段，输入数据请求者属性集合、请求份额，与访问策略中的数据集合是否匹配，匹配则可以获取属性对应的秘密，再通过不同秘密份额共同解密。

3.3　智能合约设计

本文方案主要通过智能合约实现代理重加密的密钥转换，避免第三方代理转换密钥中的隐私数据泄露，主要由以下函数完成。

密钥转换由函数ReKeyGen()实现，其中包括以下7个相关函数。首先接受患者的私钥和医生的公钥作为2个参数，函数内部通过调用Generatekeys()生成随机的公私钥，对Pri_x和Pub_x调用

PointScalarMul()使用患者的私钥与医生的公钥的标量乘法计算结果新的点Point，通过调用HashTo-curve()方法将患者私钥、医生公钥以及这个新生成的点按照一定顺序进行哈希运算得到一个在曲线上的新的点d。最后调用Bigintmul()方法，计算一个新的重新加密密钥RK，它是患者的私钥SK_P乘以点d的逆元，为保证RK在曲线范围内，对RK进行模运算。

本文方案中的智能合约均由患者调用，保证电子病历由患者控制。

4　具体方案

4.1　电子病历安全存储部分

电子病历在存储过程中，首先由区块链上的CA为患者和医生分发密钥。在诊断结束后，医生附上自己的公钥，并将病历发送给患者。患者根据自己意愿确定该病例是否进行共享，将对电子病历进行离线或者在线加密。通过智能合约，在传入医生公钥和患者私钥的基础上进行密钥转换。患者将获得转换后的重加密密钥，用于电子病历重新加密，加密文件并将其存储在IPFS中。IPFS会生成一个哈希地址，并将该地址返回给患者。患者将该哈希存储在区块链上，以便转诊时供其他医生共享。电子病历存储流程如图2所示。

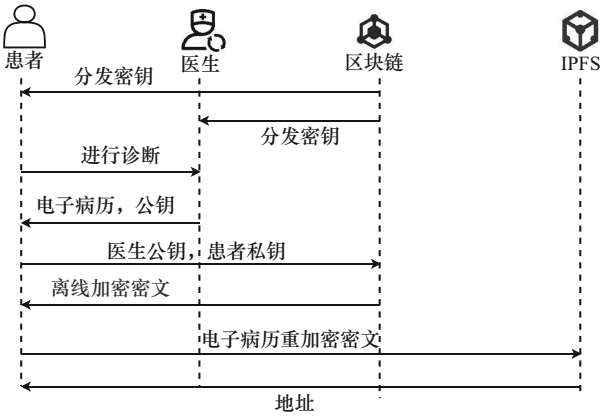

图2　电子病历存储流程

阶段1　系统初始化

$\text{setup}(1^k)\rightarrow(\text{param},\text{Msk})$。患者和医生通过Hyperledger Fabric中的CA认证，生成系统公共参数param和主密钥Msk。输入安全参数1^k，系统初始化，选取2个阶数都是大素数p的乘法循环群G_1,G_2，选择G_1的一个生成元q，设双线性映射为$e:G_1*G_2\rightarrow G_2$；随机选择$g\epsilon Z_p^*$和$u\in G_1$，有$q_1=q^g$，并且随机选取3个抗碰撞哈希函数$H_1:\{0,1\}\rightarrow G_1$，$H_2:G_2\rightarrow G_1$，$H_3:\{0,1\}\rightarrow G_2$。设置系统主密钥为Msk = s，公共参数为param = $\{q,q_1,u,e,H_1,H_2,H_3\}$。

阶段2　密钥生成

$\text{Keygen}(\text{param},\text{Msk},\text{Id})\rightarrow(\text{PK}_{\text{Id}},\text{SK}_{\text{Id}})$。CA通过系统输出的主密钥Msk和身份$\text{Id}\in\{0,1\}^*$，基于椭圆曲线数字签名算法生成医生和患者的公钥和私钥对。为系统中的数据需求者(医生)和数据所有者（患者）生成相应的公钥和私钥对。

随机选择$a,b\in Z_P^*$，计算$\text{PK}=\text{param}^{(a,b)}$，其中私钥为$\text{SK}=(a,b)$。

医生的公私钥对为$\text{Doc}(\text{PK}_D,\text{SK}_D)$。

患者的公私钥对为$\text{Pat}(\text{PK}_P,\text{SK}_P)$。

密钥生成基于离散对数问题的困难性，因为找到a,b，即g_1^a, g_1^b的指数难以计算，足以保证私钥的安全性。

阶段3　重加密密钥生成

$\text{KeyGen}_{\text{Re}}(\text{SK}_P,\text{PK}_D)\rightarrow\text{RK}_{P\rightarrow D}$。密钥转换过程是为了保证在解密阶段不需要医生和患者交换私钥解密电子病历，因此通过输入患者的私钥和医生的公钥，生成一个新的密钥PK，用于密文的重新加密。如计算$\text{PK}=\text{SK}_P\left[H_3(g^x\|\text{PK}_D\|\text{PK}_D^X)\right]^{-1}$，首先计算$g^x$、$\text{PK}_\text{D}$和$\text{PK}_\text{D}^\text{X}$的哈希值，取其逆，然后与发送者的私钥相乘。

具体步骤如下：输入参数患者私钥SK_P解析为一对整数$(a_P,b_P)\in Z_P^*$；将医生公钥PK_D解析为一对群元素$\left(\text{PK}_{D,1},\text{PK}_{D,2}\right)$；使用解析得到的参数，计算重新生成的密钥$\text{PK}=\text{PK}_{D,2}^{a_P}=g_1^{b_D a_P}$。

这样生成的RK可以用于后续的重新加密操作，以便于在密文的传递或存储过程中更新密钥而不必暴露原始的私钥信息。

阶段4　电子病历加密

1) 离线加密

$\text{Encrypt}_{\text{off}}(\text{PK}_P,m,t)\rightarrow m'_{\text{off}}$。患者对自己的病历使用个人公钥加密输出离线加密密文m'_{off}，在自己需要查看时能够方便查看。该部分为患者根据其公钥加密电子病历生成电子病历离线加密密文，具体算法为：将患者的公钥PK解析为$(\text{PK}_1,\text{PK}_2)\in G_T*G_1$，并选择随机数$k\in Z_P^*$，分别进行一级和二级加密，返回一级密文$m_1=g_2^k,m\text{pk}_1^k=mZ^{ak}$，返回二

级密文 $m_2=(e'(pk_2,g_2)^k=Z^{bk},mZ^k)$，最终生成密文 $m'_{\text{off}}=(m_1,m_2)$。该部分密文电子病历为患者不允许共享的部分，由患者自己保存。

2) 在线加密

$\text{ReEncrypt}_{\text{on}}(m'_{\text{on}},\text{PK}_{P\to D})\to m''$。在线加密部分，该部分允许共享。根据患者公钥进行离线加密电子病历，将加密后的电子病历通过重代理加密密钥再次加密后存储，一方面保证其安全存储，另一方面能够使生成病例的医生用自己的私钥查看。输入重加密密钥、离线加密的密文和患者公钥，将 m'_{off} 解析为 (m_1,m_2)，PK 解析为 $(\text{PK}_1,\text{PK}_2)\in G_T*G_1$。选择 $k'\in Z_P^*Z$ 进行重新随机化，并返回在线加密密文 $m'_1=e'(\text{RK},m_1g_2^{k'})$，$m'_2=m_2\text{PK}_1^{K'}$，$m'_{\text{on}}=(m'_1,m'_2)$。

基于智能合约的代理重加密算法1所示。通过输入患者私钥和电子病历，根据是否允许共享，进行在线加密和离线加密。如果不允许共享，患者通过自己的公钥加密，仅自己可查看。如果允许加密，首先通过患者公钥和该条件进行加密。然后输入患者私钥和该医生的公钥，进行密钥转换，得到转换后的密钥，并对第一次加密的密文进行重加密。患者将重加密的电子病历存储在IPFS中，将返回的IPFS地址存在区块链上，同时保留病历摘要和块头给患者。

算法1　代理重加密算法

输入　PK_P，PK_D，m

输出　块哈希 H 和摘要 c

1)患者收到医生诊断结果

2)患者决定是否共享

3) $f(t=0)$ //t=0是不同意共享

4)　$m'_{\text{off}}\leftarrow E(\text{PK}_P,m)$

5)　返回在线加密密文 m_{off}'

6) $\text{RK}\leftarrow \text{R}(\text{SK}_P,\text{PK}_D)$

7) $m'_{\text{on}}\leftarrow E(\text{PK}_P,m)$

8) $m''\leftarrow E(m'_{\text{on}},\text{RK})$

9)将 m'' 存入IPFS中，返回 H_{IPFS}

10)将IPFS地址打包存在区块上

11)返回块头哈希 H 和摘要 c 给患者

阶段5　解密电子病历

在该部分，解密电子病历时，患者可以通过自己的私钥解密，同时医生也可以通过自己的私钥解密，中间没有密钥交换，均可以解密密文。

1) 对于不共享的电子病历解密，患者输入自己的私钥和密文，将秘密密钥sk解析为 (a,b)。并解析 $m_{\text{off}}'=(m_1,m_2)\in G_2\times G_T$，返回 $m=\dfrac{m_2}{e'(g_1,m_1)^a}$。

2) 对于共享的电子病历，生成病历的医生输入自己的私钥，解密步骤为将 m_{on}' 密文解析为 $m_{\text{on}}'=(m_1',m_2')\in G_T^2$，计算得到并返回 $m=\left(\dfrac{m'_2}{m_1'^{\frac{1}{b}}}\right)$。

患者解密电子病历的算法2所示。患者在需要查看以往病历时，首先通过检索IPFS地址获取被加密的病历，然后通过输入自己的私钥解密电子病历。

算法2　患者解密算法

输入　SK_P，IPFS地址

输出　电子病历

1) 通过IPFS地址查询

2) if ($\text{Hash}_{\text{ipfs}}$ = true)//地址存在

3)　　返回加密的 m_{off}'

4)　　$m'\leftarrow D(m'_{\text{off}},\text{SK}_P)$

5)　　return m

6) return false

算法3为医生解密算法。在同一家医院、同一位医生处再就诊时，如果有查看以往电子病历的需求，医生会依据病历摘要向患者请求获取电子病历地址，如果该病例在可查的范围内，可以查询到IPFS地址，如果该病例无查看权限返回False，在医生获取到电子病历密文后，通过输入自己的私钥就可以解密获取电子病历。

算法3　医生解密算法

输入　SK_D,c

输出　电子病历

1) if ($c\in C$)//根据 c 检索获取IPFS地址

2)　　return $\text{Hash}_{\text{ipfs}}$

3)　　if ($\text{Hash}_{\text{ipfs}}$ = true)//地址存在

4)　　返回加密的 m''

5)　　$m\leftarrow D(m'',\text{SK}_P)$

6)　　return m

7) return false

4.2　电子病历可控共享部分

医生向区块链中的认证机构发送自己的属性，

并获取属性密钥。这一步确保了医生的身份和权限得到验证和授权。患者利用Asmuth-Bloom秘密共享算法，通过构造同余方程进行秘密分发。在这个过程中，所谓的秘密对应患者存储的以科室为单位中多位医生按照时间顺序生成的病历IPFS地址所在的特定区块链中并附有相应标签。患者设定了详细的访问策略，明确规定了哪些医生或同行可以访问病历的哪些部分。这种精细的控制机制不仅保障了病历数据的安全共享，也保护了患者的隐私信息。当数据请求者，通常是同一类型科室的医生，需要访问电子病历时，根据患者所设定的访问控制策略，获取存储在区块链上的IPFS哈希地址。数据请求者在IPFS上获得密文，并通过合作的方式，根据不同的秘密分享者，重构出电子病历的完整信息。这个过程保证了数据请求者能够合法而安全地获取电子病历明文。电子病历共享流程如图3所示。

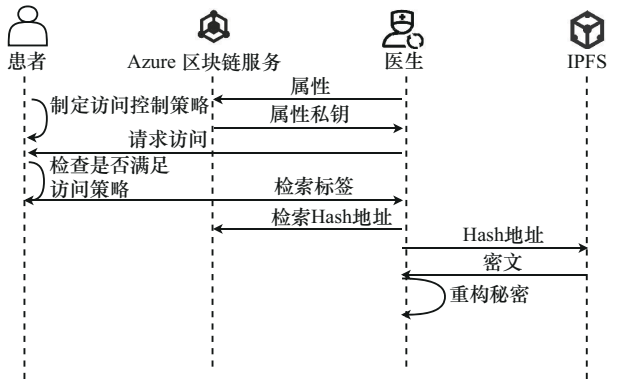

图3　电子病历共享流程

阶段1　初始化阶段

联盟链上的可信机构CA执行初始化操作，生成系统公共参数和系统主密钥。

生成一个P阶双线性群G_1，以g为其生成元，p为素数。

选择随机数$\alpha,\beta \in Z_P$,计算得公共参数$\mathrm{PK}=(G_1,g,g^{\beta},g^{\frac{1}{\beta}},e(g,g)^{\alpha})$和系统主密钥$\mathrm{MK}_S=(\beta,g^{\alpha})$。

阶段2　密钥生成阶段

本文方案中设置联盟链的参与方，对于每个参与方，属性密钥生成算法根据其属性集合生成相应的属性密钥。每个参与方都有一组属性，这些属性可能包括其身份信息、角色、权限等，这些属性是访问策略的基础，用于定义哪些参与方有权访问特定的加密数据。在该阶段，由CA完成。CA验证参与方的身份和属性信息，并基于这些信息生成相应的属性密钥。这样做可以防止恶意参与方获取未经授权的密钥，并确保只有合法的参与方能够获得有效的属性密钥。属性密钥是用于解密加密电子病历的关键，只有拥有与访问策略相匹配的属性密钥的参与方才能成功解密数据，具体如下。

数据请求者的属性m均属于属性集合S，随机选择$\varepsilon_m \in Z_P$；计算得用户属性私钥$\mathrm{SK}_{\mathrm{Attr}}=(g^{\left(\alpha+\frac{1}{\beta}\right)},\forall m \in S:g^{\varepsilon}H(m)^{\varepsilon m},g^{\varepsilon m})$。

阶段3　访问控制策略设置

患者使用CP-ABE算法对电子病历进行属性加密，生成密文。CP-ABE加密的结果基于访问策略，这个策略基于参与方的属性集合，只有满足访问策略定义的属性条件的参与方才能解密数据。

首先，设置访问控制树Γ。构建该树，每个叶子节点存储由患者设定的属性值，每个属性值对应素数。父节点给该叶子节点的秘密值也存储在相应的节点中。

其次，设置门限值(t,n)来表示某非叶子节点与其子节点之间的逻辑关系。t=1时，该节点为或门；t=n时，表示与门。这些门限值决定了解密所需的属性的数量以及它们之间的逻辑关系。

患者定义一个访问策略，旨在控制谁能够访问这份电子病历。树形结构中，根节点表示OR操作，子节点表示AND操作。每个AND节点下有2个子节点，分别表示2个属性的条件。第二个节点是一个单独的属性节点，表示单独的属性条件。如例1所示，树形结构描述了访问策略，它要求满足以下一种：1) 医生的科室为心脏病学且职务为主治医师；2) 医生的研究领域为心律失常。

例1　访问控制策略举例

OR

　AND

　　属性1：科室 = “心脏病学”

　　属性2：职务 = “主治医师”

　属性3：研究领域 = “心律失常”

当医生尝试访问电子病历时，系统会检查医生的属性是否满足树形结构中的条件。只有当医生的属性满足任一叶子节点的条件时，才允许获取解密权限。

阶段4　属性加密

属性加密过程中，由患者制定的访问控制策略

和系统公钥对相关属性对应的密钥进行加密，计算属性密文

$$C=(T,C_1=C(g,g)^{\alpha r},C=h^r,\forall y\in Y:C_y=g^{q_y(0)},C_y'H(\mathrm{att}(y))^{q_y(0)})$$

其中，r是根节点处隐藏的值，是从Z_p中随机选择的，进行属性加密时通过$\forall y\in Y:C_y=g^{q_y(0)},C_y'H(\mathrm{att}(y))^{q_y(0)}$对叶子节点操作，给每个属性计算一个值，通过哈希运算将叶子节点与某属性关联。

阶段5　秘密分发

患者利用Asmuth-Bloom秘密共享算法将加密密钥分割成多个共享部分，并将这些部分按照门限要求分发给特定数量的医生。每个医生的解密密钥作为子密钥，需要与其他参与方合作才能还原完整的密钥以解密数据。加密后的数据将被分发给符合访问策略并满足相应属性要求的参与方。参与方只能整合其属性匹配的部分密钥，而无法获取其他不匹配属性的密钥。

在本文方案中，患者的病历集合中按照科室分类，并将每个科室的所有医生的密钥设置为多个秘密分别为$c_1,c_2,\cdots,c_n,c$和C，此处满足$C=c_1+c_2+\cdots+c_n+c$，且c_i及C均为正整数，其中C为该病人某科室的完整病历的密钥，一般情况下不会有恢复的需求，在特殊情况下需要恢复使用。

假设$C=\{C_1,C_2,\cdots,C_m\}$是$\{1,2,\cdots,n\}$的一个分割，分类门限序列为$K=\{k_1,k_2,\cdots,k_n\}$。

当$1\leqslant k_j\leqslant\left|C_j\right|$时，对于所有$1\leqslant j\leqslant m$和一个整体门限$k(\sum_{j=1}^{m}k_j\leqslant k\leqslant n)$，有$(C,K,k)$分类接入结构表

$$A=\{A\in P(\{1,2,\cdots,n\})(|A|\geqslant k)\wedge(\vee j=1,2,\cdots,m)(\left|A\cap C_j\right|\geqslant k_j)\}$$

具体为，n为一个整数，有$2<k<n$，给定正整数序列，在本文方案中将完整的解密密钥作为秘密处理为正整数$m_1<m_2<\cdots<m_n,(m_i,m_j)=1$，$1\leqslant i<j<n$，如果满足$m_{n-k+2}m_{n-k+3}\cdots m_n<m_1m_2\cdots m_k$，那么就能够构建$(k,n)$序列，根据$I_i=S(\mathrm{mod}\,m_i)$，得到秘密份额$I_i$，并按照属性策略配对，也就是每个属性对应一个子秘密。

阶段6　秘密恢复

再就诊时的主治医生即参与方想要访问加密数据，首先需要检查其属性集合是否满足访问策略的要求。只有当参与方拥有访问策略所需的属性密钥，并且获得了足够数量的子秘密时，参与方需要进行秘密重构。一旦参与方获得了解密电子病历密钥的所有必要部分，他们就可以将这些部分合并，解密还原出完整的病历。解密后的数据可以被参与方访问和使用，从而实现了数据共享方案中对加密数据的安全共享和访问控制，具体流程如下。

在解密叶子节点的过程中，医生的属性集合需要包含与该节点属性值相匹配的属性。医生可以利用这些匹配的属性来解密当前节点的秘密。

解密叶子节点时，医生可能会获得多对对应值，通过逐层解密并依次类推的方式，逐步获取父节点的秘密。这个过程类似于逐级解锁的方式，直到达到根节点或者满足了所有门限值的要求。在获取K组不同的秘密份额时，此处用$I_{i_1},I_{i_2},\cdots,I_{i_k}$表示，当这些参与者提供自己保管的秘密时，建立以下方程组，可以根据算法进行秘密重构法获取需要的病历。

$$\begin{cases}x=I_{i_1}(\mathrm{mod}\,m_{i_1})\\x=I_{i_2}(\mathrm{mod}\,m_{i_2})\\\quad\vdots\\x=I_{i_k}(\mathrm{mod}\,m_{i_k})\end{cases}$$

5　安全性分析

5.1　Hyperledger Fabric平台安全性分析

Hyperledger Fabric 使用基于 X.509 标准的证书进行身份认证。每个参与者都有一个唯一的身份，由CA颁发。在该平台中，通过数字证书标识网络中的每个参与者，具有独特性。其中的链码通过容器化技术隔离运行，并受到安全性审计和限制，能防止恶意攻击行为或篡改代码的影响。

共识机制是可插拔的，Kafka是Fabric默认的共识算法，但是在此共识模式之下，节点通信过程，如果集群出现故障或性能问题，可能会影响到整个区块链网络的运行。维护Kafka集群复杂性高、成本大，特别是在医疗领域，安全性和稳定性要求高，需要投入更多的资源来确保系统的稳定运行。此外，在处理大量的医疗交易时，可能会引入一定的性能开销。这可能会影响到电子病历共享平

台的实时性和响应性能，因此本文方案中选择实用拜占庭容错共识机制（PBFT），因为拜占庭的共识机制能够容忍一定数量的恶意节点，并且对于系统中存在的少数节点的故障和攻击，PBFT仍然能够达成一致的共识，保证一定的容错性。PBFT允许多个顺序服务节点互相协作，共同验证和排序交易，还能够通过使用复杂的消息交换和同步协议保证节点间的一致性，防止恶意节点篡改交易和拒绝服务等攻击，保证用户的数据和交易安全。

5.2 病历存储安全性分析

本文方案主要使用代理重加密算法，将电子病历信息进行加密并保护。在加密过程中，采用随机数和时间戳等措施防止攻击者重复使用已截获的密文，确保每次加密操作都是独一无二的，从而避免了密钥泄露的风险，确保明文电子病历不会被泄露。加密后的电子病历数据存储在IPFS中，并通过唯一的Hash地址进行查询。IPFS作为一种结合了分布式哈希表的存储系统，当存储的内容发生变化时，其地址也会相应改变，因此可以通过返回的不同地址来检查密文是否发生了改变，从而保证电子病历的完整性。此外，IPFS采用快照模式来存储文件变更，每次提交都会生成一个快照，而不是保存文件的差异，这在处理大型代码库和跟踪文件变更时更加高效和灵活。IPFS的分布式存储方式使得数据分散在网络中的多个节点上，而非集中存储在单一位置，从而降低了系统被单点攻击的风险。

5.3 病历共享安全性分析

密钥转换通过智能合约完成，并部署在区块链上，避免了第三方密钥转换的问题。智能合约在虚拟机中运行，提供了隔离性和计算结果的共识验证，确保了计算的可信性。通过这种方式，确保了病历数据在共享过程中不会因密钥交换而导致泄露。参与秘密分发的各方协作恢复密钥，以解密病历，从而确保只有授权人员能够访问病历数据。

5.4 抗攻击性分析

5.4.1 抗篡改攻击

该攻击指攻击者对系统中的数据进行非法修改或篡改的行为。这种攻击可能会导致数据的完整性受损，使得系统中的信息不再可信。本文方案能够抵御篡改攻击，任何人尝试更改病历内容，都会产生一个新的IPFS地址，并将这个地址与相应的病历记录关联起来，然后将这个关联记录写入区块链中。即使攻击者尝试篡改病历内容并修改IPFS地址，也无法篡改已经写入区块链中的记录，因为区块链的特性确保了数据的不可篡改性，这个修改将无法被覆盖或隐藏，从而确保了病历数据的完整性。

5.4.2 抗拒绝服务攻击

拒绝服务攻击是指攻击者通过向目标系统发送大量请求或者占用系统资源，导致目标系统无法正常提供服务或者响应请求的一种网络攻击行为。本文方案使用Hyperledger Fabric平台，包括分布式共识机制，通过多个节点的共同验证来达成一致性。关键信息存储在多个节点上，即使部分节点受到攻击，系统仍能保持运行，降低了遭受DoS攻击的风险。CA能提供身份验证和授权机制，只允许经过授权的用户或节点访问系统资源，防止未经授权的访问和恶意行为，使得系统更加鲁棒。

5.4.3 抗身份伪造攻击

该攻击指攻击者试图冒充他人的身份或者实体，以获取未经授权的访问权限或者执行恶意活动。在身份伪造攻击中，攻击者通常试图获取目标系统中合法用户或者系统实体的权限，并以其身份进行活动，以达到不正当的目的。该方案中，CA负责颁发数字证书，确保参与系统的医生或者患者都拥有唯一的身份标识，并验证其身份。因此这种机制可以有效防止攻击者伪造身份或者获取未经授权的访问权限。

5.4.4 抵御隐私泄露

本文方案在病历生成后根据共享情况进行加密。对于不共享的病历，采用基于椭圆曲线的数字签名算法，这种非对称加密方法确保了加密和解密过程中使用的密钥不同，其安全性经过广泛验证。在密钥转换过程中，计算$\mathrm{RK}=\mathrm{SK}_P\cdot\left[H_3\left(g^x\|\mathrm{PK}_D\|\mathrm{PK}_D^X\right)\right]^{-1}$对患者私钥、医生公钥以及随机数进行指数运算后再进行哈希运算，从而使攻击者无法推算出患者私钥或随机数的值。对于重加密后，医生访问时通过自己的私钥解密，不需要进行密钥交换，在密钥管理角度安全。因此本文方案可以确保病历数据在传输和存储过程中不被未授权的用户获取，有效地防止隐私泄露事件的发生。通过加密，即使数据被截获或存储介质被盗取，未经授权的用户也无法解密和访问其中的敏感信息，保障了数据的机密性和完整性。

5.5　Asmuth-Bloom秘密共享方案安全性分析

首先，本文中的Asmuth-Bloom方案的安全性依赖于门限密钥重构算法。在该算法中，参与方必须合作才能重构出完整的秘密。理论上，只有当参与方拥有足够数量的秘密部分时，才能够重构出完整的秘密。这种门限要求的安全性可以通过数学证明得到验证。

假设对于某一非授权子集，存在2种情况：第一种，若非授权子集小于门限序列$|A|<k$，秘密无法被恢复；第二种，若病历科室分类存在$\left|A\cap C_j\right|<k_j$，秘密无法被恢复。

其次，本文的Asmuth-Bloom门限方案使用了多项式取模运算和同余方程组求解等数学原理来实现秘密分割和重构。在这个过程中，多项式取模运算涉及到在有限域上进行计算，通常基于大素数的算术运算。在这些运算中，依赖的主要是离散数学中的2个难题。

大素数分解问题：这个问题是指将一个大的合数分解为其素因子的问题，虽然在理论上，任何合数都可以被分解为素因子，但对于非常大的合数，目前的计算技术使得分解变得极其困难。

离散对数问题：这个问题是在有限域上进行的，即在模数下进行的指数问题。给定一个生成元g和一个元素h，找到使得$g^x=h(\mathrm{mod}\,p)$，成立的x的值。在素数域上进行的离散对数问题通常是困难的，特别是当素数p很大。

最后，本文提出的电子病历共享方案整个过程中主要是采用CP-ABE其安全性基于判断性PBDHE数学难题，已经过证明在标准模型下的安全性，获取密文在区块链上查找对应IPFS，因Hyperledger Fabric分布式账本造假篡改恶意访问均可查可证，可以保证其共享安全性。

本文方案中的Asmuth-Bloom算法的正确性主要基于中国剩余定理，该定理可以确保，在只知道一组模的不同余数集合时，仍然可以求出一个整数，该整数对于每个都能满足，因此在收集足量参与者与其大素数对，即可构造出原始秘密。选择足够大的素数保证取值不会泄露秘密信息。因为素数足够大，可知计算困难，故不会泄露秘密，保证算法安全性。

综上所述，Asmuth-Bloom秘密共享方案的安全性建立在门限安全性、多项式取模运算安全性之上。

6　性能分析

6.1　理论分析

6.1.1　功能对比

本文方案旨在解决电子病历过程中的病历归属权不清晰、病历共享不受控等问题，与已有的电子病历共享方案[24-27]进行对比，如表2所示。较文献[24,27]而言，本文方案是基于属性的，在医疗信息共享过程中允许根据用户的属性或角色来定义访问策略，从而实现对数据的细粒度访问控制，并且允许根据应用场景和需求来定义访问策略，因此非常灵活，且病历的授权者为患者和部分医生，一方面患者掌控自己的所有病例，另一方面诊断医生也能参与自己生成病例的管理，满足实际需求；较文献[25-26]而言，本文方案能够允许多各机构的共享，共享范围较大满足电子病历共享在应用场景中的需求，并且较私有链服务器授权更简洁，在实际场景中更具适用性。

6.1.2　时间复杂度对比

将Asmuth-Bloom秘密共享算法应用在电子病历的共享中，实现对电子病历的细粒度访问控制。在部分医疗信息共享的解决方案中，涉及其他秘密共享算法（如表3所示）。文献[25]提出的LSSS线性秘密共享方案使用Lagrange插值多项式，其时间复杂度可估计为$O(k\log^2 k)$；文献[27]提出的Ro-

表2　各方案功能对比

方案	隐私保护	共享机构	基于属性	控制方式	授权者	病例请求灵活性
文献[24]	是	多机构	否	可搜索加密	私有链服务器	较灵活
文献[25]	是	单个	是	线性秘密共享	机构授权	不灵活
文献[26]	是	单个	是	可搜索加密	自动	不灵活
文献[27]	是	—	否	智能合约	自动	固定
本文方案	是	多机构	是	Asmuth-Bloom秘密共享	患者和部分医生	任意份病历

表3 各个秘密共享方案的时间复杂度

方案	秘密共享算法	时间复杂度	说明
文献[28]	改进的Robust秘密共享方案	$O(kn^{\varepsilon})$	ε是常数
文献[27]	Robust 秘密共享方案	$O(k\text{ploy}\log(n))$	$\text{poly}\log(n)$是多项式对数函数
文献[29]	Shamir秘密共享方案	$O(k\log^2 k)$	—
文献[25]	线性秘密共享	$O(k\log^2 k)$	—
本文方案	Asmuth-Bloom秘密共享算法	$O(k)$	k是参与者个数

bust秘密共享方案是改进的文献[28]方案，是一种基于多线性映射的秘密共享方案，多线性映射可能会导致较高的计算复杂度；文献[29]中的Shamir秘密共享算法，由Lagrange插值多项式实现，其时间复杂度为$O(k\log^2 k)$。尤其是在处理大规模数据时，会增加系统的运行成本和时延，其时间复杂度为$O(kn^{\varepsilon})$；Asmuth-Bloom秘密共享算法是根据中国剩余定理实现，其时间复杂度为$O(k)$。与其他几种秘密共享算法相比，Asmuth-Bloom秘密共享算法根据中国剩余定理实现，在恢复秘密时需要处理k个同余方程，其时间复杂度为$O(k)$。据此分析，本文所采用的方案具有与参与者个数相关的时间复杂度，小于其他几种秘密共享算法。

6.2 仿真测试

本文方案在仿真测试中对加密电子病历上传到IPFS和从IPFS下载时间、加解密时间以及不同属性个数对秘密重构时间做了测试，来证明方案的可行性。

通过压力测试工具统计了上传到IPFS和从IPFS下载不同大小的文件所需的时间，如图4所示，文件大小范围为10~85 KB。结果显示，随着文件大小的增加，上传和下载的时间都增加。由于IPFS是一个去中心化的分布式文件存储系统，上传至IPFS所需的时间略高于从IPFS下载的主要原因之一是在上传文件至IPFS时，系统需要对文件进行分块、哈希计算、加密、传输到网络中的不同节点等操作。这些过程需要消耗一定的计算资源和时间，尤其是在文件较大或网络条件不佳的情况下。另一个影响因素是网络传输的特性，上传文件时，需要将文件的数据从本地计算机传输到IPFS网络中的节点，而下载文件时，数据则是从IPFS网络中的节点传输到本地计算机。通常情况下，上传速度受到本地网络上传带宽的限制，而下载速度则受到IPFS网络中节点的响应速度和网络带宽的限制。由于网络的不确定性和不同节点之间的连接情况不同，上传速度可能会稍高于下载速度。但是总体而言时间仍然在不影响系统效率的合理范围内。

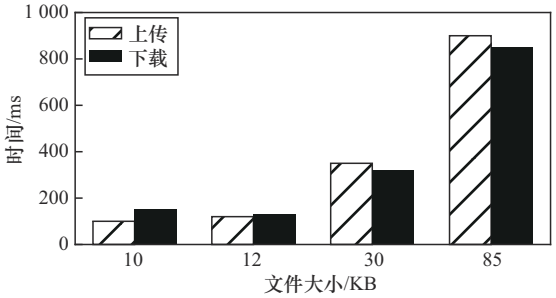

图4 上传IPFS和从IPFS下载时间

如图5所示，本文方案还对基于智能合约的代理重加密算法的加解密时间做了测试，随着文件大小逐渐增大，加密时间也相应增加。因为在本文方案中使用智能合约完成代理重加密算法，在加密过程中，双线性运算及加密算法较为复杂，且中间还有密钥转换过程中的乘运算以及指数运算造成较大的时间开销，而解密运算相对较为简单时间消耗较少。

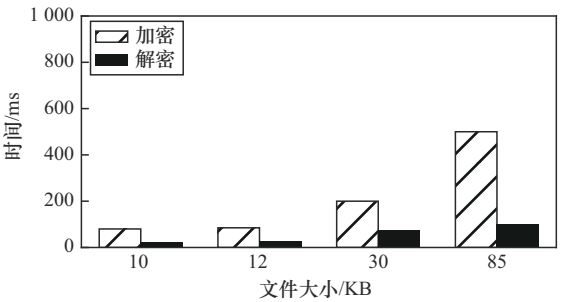

图5 加解密时间

秘密重构时间在就诊期间的电子病历共享的应用背景下显得尤其关键，在需要迅速恢复丢失的秘密或者在需要及时访问秘密信息的场景下，秘密重构时延可能导致数据丢失或系统停机时间延长，进

而对业务造成不良影响。因此，在设计秘密重构算法时，必须充分考虑秘密重构的速度和效率，以满足实际应用的需求。

本节最后对不同属性个数对秘密重构时间的影响进行了测评。如图6所示，随着属性个数的增加，秘密重构时间逐渐增加。当属性个数为4个时，秘密重构时间不到0.1 s；当属性达到12个时，秘密重构时间略超过0.2 s，随着属性个数增加重构时间增速较缓，在未来属性个数持续增加的情况下重构时间仍然在一个可接受的高性能区间。

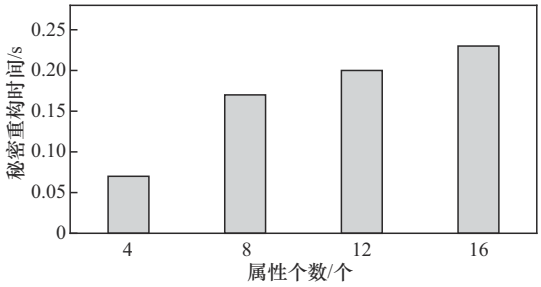

图 6　不同时间的秘密重构时间

7　结束语

本文提出的基于Hyperledger Fabric的电子病历共享方案，按照患者意愿将电子病历区分为允许共享和不允许共享部分，由患者控制，同时将代理重加密的方案通过智能合约实现，避免了第三方密钥转换不诚实的问题，将加密的电子病历存储在IPFS中保证其安全性，在解决电子病历共享的问题时，采用CP-ABE算法和Asmuth-Bloom秘密共享算法结合的方案实现多机构的可控的电子病历共享，在最后的测试中，本文方案在共享中的秘密恢复相对其他秘密共享方案有更小的时间复杂度，且相对于同类型方案更具有灵活性。未来将在撤销属性权限方面做更多的工作。

参考文献：

[1] JIN H, LUO Y, LI P L, et al. A review of secure and privacy-preserving medical data sharing[J]. IEEE Access, 2019, 7: 61656-61669.

[2] 李晓蕾, 王猛, 刘钰周. 医疗大数据隐私信息泄露途径分析及保护举措[J]. 现代计算机, 2023, 29(16): 93-98.
LI X L, WANG M, LIU Y Z. Analysis and measures of medical bigdat-privacy information disclosure[J]. Modern Computer, 2023, 29(16): 93-98.

[3] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[R]. 2008.

[4] 薛腾飞, 傅群超, 王枞, 等. 基于区块链的医疗数据共享模型研究[J]. 自动化学报, 2017, 43(9): 1555-1562.
XUE T F, FU Q C, WANG C, et al. A medical data sharing model *via* blockchain[J]. Acta Automatica Sinica, 2017, 43(9): 1555-1562.

[5] 周辉, 王丽丹, 钟成跃. 区块链助力电子医疗数据共享[J]. 解放军医院管理杂志, 2019, 26(7): 645-647.
ZHOU H, WANG L D, ZHONG C Y. Block chain facilitates electronic medical data sharing[J]. Hospital Administration Journal of Chinese PLA, 2019, 26(7): 645-647.

[6] 徐健, 陈志德, 龚平, 等. 基于区块链网络的医疗记录安全储存访问方案[J]. 计算机应用, 2019, 39(5): 1500-1506.
XU J, CHEN Z D, GONG P, et al. Secure storage and access scheme for medical records based on blockchain[J]. Journal of Computer Applications, 2019, 39(5): 1500-1506.

[7] 朱诗生, 李朝清, 黄仁俊, 等. 基于区块链的医疗数据安全共享模型与机制[J]. 计算机技术与发展, 2020, 30(10): 123-130.
ZHU S S, LI C Q, HUANG R J, et al. Secure sharing model and mechanism of medical data based on block chain[J]. Computer Technology and Development, 2020, 30(10): 123-130.

[8] 罗文俊, 闻胜莲, 程雨. 基于区块链的电子医疗病历共享方案[J]. 计算机应用, 2020, 40(1): 157-161.
LUO W J, WEN S L, CHENG Y. Blockchain-based electronic health record sharing scheme[J]. Journal of Computer Applications, 2020, 40(1): 157-161.

[9] CUI S J, ASGHAR M R, RUSSELLO G. Towards blockchain-based scalable and trustworthy file sharing[C]//Proceedings of the 2018 27th International Conference on Computer Communication and Networks (ICCCN). Piscataway: IEEE Press, 2018: 1-2.

[10] 郭庆, 田有亮. 支持受控共享的医疗数据隐私保护方案[J]. 西安电子科技大学学报, 2024, 51(1): 165-177.
GUO Q, TIAN Y L. Medicaldata privacy protection scheme supporting controlled sharing[J]. Journal of Xidian University, 2024, 51(1): 165-177.

[11] 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.
TANG F, CHEN Y L, FENG Z. Electronic prescription sharing scheme based on blockchain and proxy re-encryption[J]. Computer Science, 2021, 48(S1): 498-503.

[12] 庞震, 姚远, 张晓琴. 基于区块链的医疗数据安全存储与共享方案[J]. 信息网络安全, 2021, 21(S1): 168-172.
PANG Z, YAO Y, ZHANG X Q. Safe storage and sharing scheme of medical data based on blockchain[J]. Netinfo Security, 2021, 21(S1): 168-172.

[13] THWIN T T, VASUPONGAYYA S. Blockchain-based access control model to preserve privacy for personal health record systems[J]. Security and Communication Networks, 2019, 2019: 8315614.

[14] 李腾, 贾耀清, 贾东立, 等. 基于区块链的多客户端医疗信息共享方案[J]. 现代电子技术, 2022, 45(10): 80-86.
LI T, JIA Y Q, JIA D L, et al. Multi-client medical information sharing scheme based on blockchain[J]. Modern Electronics Technique, 2022, 45(10): 80-86.

[15] 金琳, 田有亮. 基于区块链的多权限属性隐藏电子病历共享方案[J]. 网络与信息安全学报, 2022, 8(4): 66-76.
JIN L, TIAN Y L. Multi-authority attribute hidden for electronic medi-

cal record sharing scheme based on blockchain[J]. Chinese Journal of Network and Information Security, 2022, 8(4): 66-76.

[16] 闫冠辰, 姜顺荣, 李胜利, 等. 基于联盟链的安全和支持高效模糊查询的电子病历共享系统[J]. 密码学报, 2022, 9(5): 805-819.
YAN G C, JIANG S R, LI S L, et al. Secure and efficient fuzzy search for EHR sharing based on consortium blockchain[J]. Journal of Cryptologic Research, 2022, 9(5): 805-819.

[17] 孙晓晔, 辛凤艳, 王冬艳, 等. 面向研究机构的病案共享区块链模型研究[J]. 河北省科学院学报, 2023, 40(2): 24-28.
SUN X Y, XIN F Y, WANG D Y, et al. Research on blockchain model of electronic medical record sharing for scientific research institutions [J]. Journal of the Hebei Academy of Sciences, 2023, 40(2): 24-28.

[18] BLAZE M, BLEUMER G, STRAUSS M. Divertible protocols and atomic proxy cryptography[C]//Proceedings of the Advances in Cryptology—EUROCRYPT'98. Berlin: Springer, 2006: 127-144.

[19] 陈辉焱, 刘乐, 张晨晨. 一种具有CDH问题安全性基于身份的签名方案[J]. 计算机工程, 2018, 44(4): 174-180.
CHEN H Y, LIU L, ZHANG C C. An identity-based signature scheme with CDH problem security[J]. Computer Engineering, 2018, 44(4): 174-180.

[20] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//Proceedings of the 13th ACM conference on Computer and communications security. New York: ACM Press, 2006: 89-98.

[21] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP '07). Piscataway: IEEE Press, 2007: 321-334.

[22] ASMUTH C, BLOOM J. A modular approach to key safeguarding[J]. IEEE Transactions on Information Theory, 1983, 29(2): 208-210.

[23] 贺智明, 徐亿达. 区块链与可搜索加密结合的电子病历共享方案[J]. 计算机工程与应用, 2021, 57(21): 140-147.
HE Z M, XU Y D. Electronic medical record sharing scheme based on blockchain and searchable encryption[J]. Computer Engineering and Applications, 2021, 57(21): 140-147.

[24] YANG X H, LI W J, FAN K. A revocable attribute-based encryption EHR sharing scheme with multiple authorities in blockchain[J]. Peer-to-Peer Networking and Applications, 2023, 16(1): 107-125.

[25] ZHANG L, ZOU Y, YOUSUF M H, et al. BDSS: blockchain-based data sharing scheme with fine-grained access control and permission revocation in medical environment[J]. KSII Transactions on Internet and Information Systems, 2022, 16(5): 1634-1652.

[26] MADINE M M, BATTAH A A, YAQOOB I, et al. Blockchain for giving patients control over their medical records[J]. IEEE Access, 2020, 8: 193102-193115.

[27] FEHR S, YUAN C. Towards optimal robust secret sharing with security against a rushing adversary[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2019: 472-499.

[28] LLISON B, VALERIO P, RAJMOHAN R, et al. Essentially optimal robust secret sharing with maximal corruptions[C]//Proceedings of the 35th Annual International Conference on Advances in Cryptology-EUROCRYPT. Berlin: Springer, 2016: 58-86.

[29] MAHDI G S, YOUSIF N A, SHIMAL A F. Medical image watermarking based on secret sharing and integer wavelet transform[J]. Journal of Physics: Conference Series, 2021, 1963(1): 012159.

[作者简介]

陈嘉莉（1997– ），女，宁夏固原人，宁夏大学硕士生，主要研究方向为区块链技术应用、电子病历共享等。

马自强（1990– ），男，新疆乌鲁木齐人，博士，宁夏大学副教授、硕士生导师，主要研究方向为计算机系统安全、区块链应用安全。

苗莉（1986– ），女，江苏徐州人，博士，宁夏大学讲师，主要研究方向为网络空间安全、博弈理论和边缘计算等。

李冰雨（1990– ），男，河南安阳人，博士，北京航空航天大学副教授、硕士生导师，主要研究方向为密码应用、网络认证、分布式身份、信任管理。

岳晓琳（1998– ），女，山东聊城人，宁夏大学硕士生，主要研究方向为区块链技术应用。