# 基于椭圆曲线签密的跨链医疗数据共享方案

俞惠芳，李磊
（西安邮电大学网络空间安全学院，陕西 西安 710121）

**摘　要：**去中心化区块链能实现医疗数据的存储，却因区块链对外部环境高度封闭导致医疗机构内部区块链上医疗数据只能在本机构内部共享。为了解决医疗数据在跨链共享中存在的请求者身份认证和共享数据安全等问题，提出基于椭圆曲线签密的跨链医疗数据共享方案。中继链用于实现医疗数据的交互共享。分层处理跨链医疗数据方法达到良好的共享效果。为了得到高执行效率，签密过程交由智能合约完成。针对医疗数据需要经常更改的问题，智能合约上部署了修改或删除医疗数据的操作。

**关键词：**区块链；中继链；椭圆曲线签密；分层交换；数据更改
**中图分类号：**TP309.2
**文献标志码：**A
**DOI：**10.11959/j.issn.1000−436x.2024213

# Cross-chain medical data sharing scheme based on elliptic curve signcryption

YU Huifang, LI Lei
School of Cyberspace Security, Xi’an University of Posts and Telecommunications, Xi’an 710121, China

**Abstract:** Decentralized blockchain can realize the storage of medical data. Due to high isolation of blockchain from external environments, medical data in inside blockchain of medical institutions can only be shared within institution itself. To address the requester identity authentication and shared data security in cross-chain medical data sharing, a cross-chain medical data sharing scheme based on elliptic curve signcryption was devised in this article. Relay chain was used to realize interactive sharing of medical data. Cross-chain medical data was hierarchically processed for better effect of cross-chain data exchange. Signcryption process was completed by smart contracts to obtain high execution efficiency. Deletion and modification functions of medical data were deployed in smart contracts to solve the frequent updation problem of medical data.

**Keywords:** blockchain, relay chain, elliptic curve signcryption, hierarchical exchange, data modification

## 0　引言

电子医疗数据因使用方便、存储量小、便于分析患者病情等优势在现代医疗体系中成为不可或缺的一部分[1-2]。商业利益等缘故会造成患者的医疗数据泄露。目前大多数医疗机构对于本机构就医患者的医疗数据采用集中式存储，如果存储医疗数据的服务器遭受攻击，患者医疗数据会被泄露，还可能导致医生无法读取患者医疗数据，给患者治疗造成不便。现实中医患之间极易发生医疗纠纷，患者医疗数据完全掌握在医疗机构；医疗机构为了避免责任，可能会篡改患者的医疗数据[3]，故需要找到去中心化、不可篡改的结构用来存储医疗数据。

**收稿日期：**2024–07–10；**修回日期：**2024–12–19
**通信作者：**俞惠芳，yuhuifang@xupt.edu.cn
**基金项目：**企业合作基金资助项目（No.HX2024-002, No.HX2024-297）
**Foundation Items:** Enterprise Cooperation Projects (No.HX2024-002, No.HX2024-297)

区块链在电子医疗领域发挥了极大作用[4]，能很好地保护病人隐私，防止医疗数据被篡改。通常使用加密算法处理区块链上医疗数据，没有解密权限的用户不能解密被截获的密文。区块链可通过智能合约或其他权限管理机制严格控制数据的访问和操作，访问权限管理系统使得只有授权用户可解密和查看数据。现实中患者往往不会在同一个医疗机构就诊，为了得到患者既往病史，就需要在医疗机构之间共享数据。然而，由于区块链结构本身局限性导致记录在区块链上的数据只能在医疗机构内部共享[5]。

为了解决区块链上医疗数据的孤岛问题，跨链医疗数据共享机制值得被研究。文献[6]提出的医疗数据管理方案，可促进电子病历共享流程，全部医疗数据存储在联盟链上却增加了链的存储压力。文献[7]提出了关键字密文检索的电子病历双重授权方案，医疗数据的密文存储在云服务器上，病历关键词索引上传至区块链，医院控制区块链上病历关键字检索权限，患者用代理重加密控制病历的解密权限，实现了医院和患者对共享病历的双重授权。文献[8]构建了访问控制模型，边缘服务器中数据的提取记录存储在联盟链上，医疗数据存储在文件服务器中，没有电子病历被大量恶意访问的现象。文献[9]提出的区块链下可搜索加密方案，可降低医疗数据共享中的计算开销。文献[10]提出的分布式个人健康记录共享方案能快速加解密，区块链以交易形式记录针对数据的所有操作。基于关键字可搜索加密的医疗数据共享方案[11]能更好认证数据请求者身份，解决了属性加密中显式访问策略匹配会泄露病人隐私的问题，属性和访问策略匹配时属性向量和访问策略向量做内积即可。文献[12]提出基于椭圆曲线签名的区块链电子病历共享方案，解决了通用验证者签名证明效率低的问题。文献[13]使用每个电子病历的会话密钥，防止医生访问不相关的电子病历。上述方案都是集中存放医疗数据的，以区块链为基础进行数据共享，大量的数据请求无疑会增加区块链的计算压力；同时在医疗数据共享中没有根据病人实际情况区别处理，导致医疗数据共享过程的实用性不高。

本文提出无证书体制下[14]基于椭圆曲线签密的可支持患者医疗数据修改的跨链医疗数据共享方案。中继链[15-16]负责收集、验证、传递医疗数据到区块链上，两个链通过通道内数据结构实现跨链数据共享，保证跨链共享数据的真实性，并解决智能合约在执行过程中对外部数据的依赖。签密过程交由智能合约执行使计算效率得到极大提高。分层处理不同跨链请求，实现了跨链医疗数据的共享。本文方案可保护患者的隐私数据，降低医疗数据在传输中的计算复杂度，随着患者的病情发展可对医疗数据进行更新或删除。

## 1 椭圆曲线密码

给定大素数$Q$阶的有限域$\mathbb{F}_q$，$\mathbb{F}_q$上定义椭圆曲线$E$：$y^2 = x^3 + ax + b \bmod Q$（$a$,$b$都是小于$Q$的非负整数，$4a^3 + 27b^2 \bmod Q \neq 0$）。假设$O$是$E$的无穷远点，$G$是$E$的基点，$q$是点$G$的素数阶，$qG = O$。椭圆曲线点$E(a,b)$和$O$形成$q$阶的循环加法群$\mathbb{G} = (x,y):x,y \in \mathbb{F}_q,(x,y) \in E(a,b) \cup O$。

椭圆曲线Diffie-Hellman（ECCDH）问题：给定$E$上两点$Y = aG(a < q)$，$X = bG(b < q)$，计算$\omega = abG(a,b < q)$。

椭圆曲线离散对数（ECDL）问题：给定$E$上的点$Y = aG(a < q)$，计算$a < q$。

## 2 跨链系统模型

基于本文方案的跨链系统模型如图1所示。具体如下：系统管理中心负责公布系统的公共参数，核实新加入医疗机构的资质且为所在区块链分发系统内唯一身份标识，通知系统内的所有医疗机构。区块链中存储的信息包含本医疗机构中患者身份信息和星际文件系统（IPFS, interplanetary file system）中医疗数据密文的地址密文。中继链负责审核、记录、转发跨链请求，针对跨链请求进行路由选择。跨链网关对接加入系统的区块链，转发区块链的跨链请求到中继链上，转发从中继链到数据链的消息。IPFS存储患者医疗数据的密文，返回地址给区块链智能合约。

## 3 本文方案

### 3.1 初始化算法

1) 系统管理中心随机选取$\mu$比特大素数$Q$，定义$\mathbb{F}_Q$上的椭圆曲线$E$；选择具有素数阶$q$的椭圆曲线$E$的基点$G$，$G$也是具有素数阶$q$的加法循环群

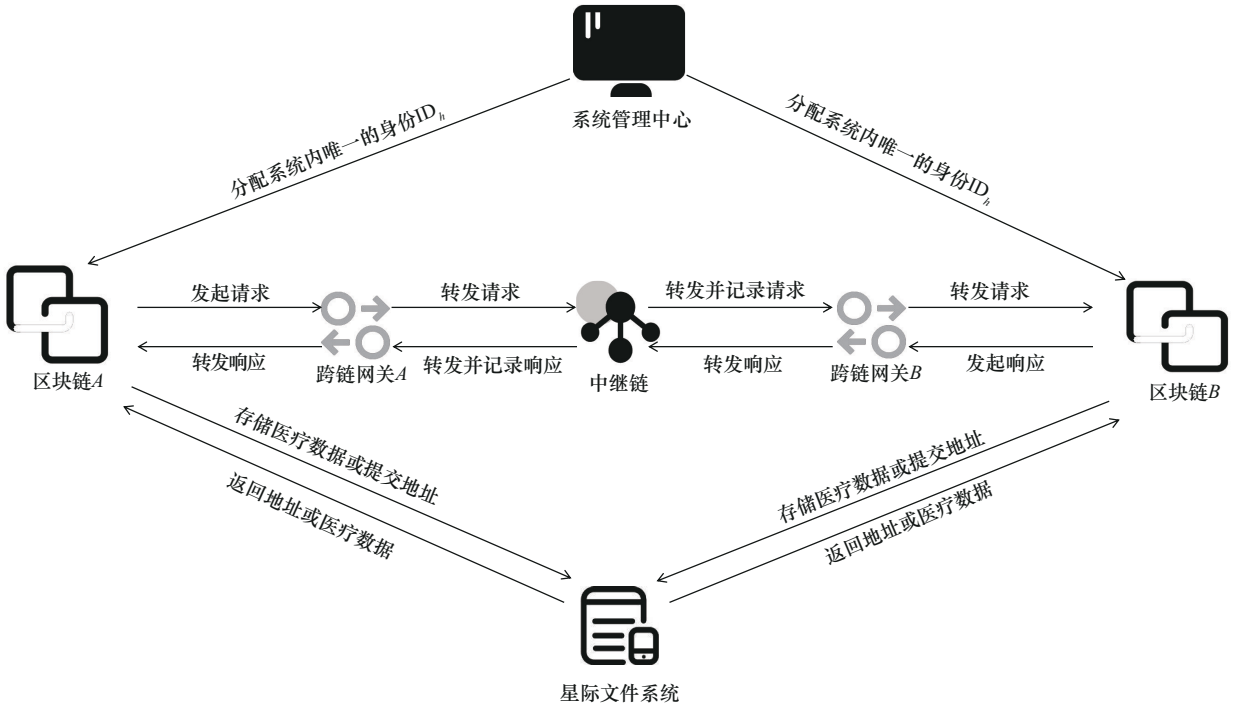


图1　基于本文方案的跨链系统模型

$\mathbb{G}$ 的生成元。然后，选取系统的主控钥 $s \in \mathbb{Z}_q^*$，计算系统公钥 $y_{\text{pub}} = sG$。

2) 系统管理中心选取安全哈希函数 $H_1:\mathbb{G} \times \{0,1\}^{L_1} \to \mathbb{Z}_q^*$（$L_1$ 是医疗机构、医生和患者身份信息的长度），$H_2(H_4):\mathbb{G} \times \mathbb{G} \to \{0,1\}^{L_2(L_R)}$（$L_2$ 是 IPFS 存储地址密文的长度，$L_R$ 是患者申请消息 $R_p$ 的长度），$H_3(H_5):\{0,1\}^{L_2(L_R)} \times \mathbb{G} \to \mathbb{Z}_q^*$，$H_6:\mathbb{G} \times \mathbb{G} \to \{0,1\}^{L_R+L_R}$，$F:\mathbb{G} \to \{0,1\}^{L_3}$（$L_3$ 是对称密钥的长度）。

3) 系统管理中心公开系统全局参数 $\pi = <Q,\mathbb{F}_Q,q,E,G,\mathbb{G},y_{\text{pub}},H_1,H_2,H_3,H_4,H_5,H_6,F>$。

### 3.2　公私钥生成算法

1) 医疗机构管理者选择私钥 $x_h \in \mathbb{Z}_q^*$，计算公钥 $y_h = x_hG$，向本系统内医疗机构公布公钥 $y_h$。

2) 医生 $\text{ID}_d$ 选择私钥 $x_d \in \mathbb{Z}_q^*$，计算公钥 $y_d = x_dG$，随后在本系统内公布公钥 $y_d$。

3) 患者 $\text{ID}_p$ 首次在医院治疗时选取私钥 $x_p \in \mathbb{Z}_q^*$，计算公钥 $y_p = x_pG$，治疗时出示公钥 $y_p$。

### 3.3　部分公私钥生成算法

医疗中实体向系统管理中心申请部分公私钥。系统管理中心选择随机数 $d_i \in \mathbb{Z}_q^*$，计算 $Y_i = d_iG$，$\varphi_i = H_1(y_i,\text{ID}_i)$，$X_i = \varphi_i s + d_i \bmod q$。然后，向医疗实体发送部分私钥 $X_i$。实体可通过 $X_iG = \varphi_i y_{\text{pub}} + Y_i$ 验证部分私钥的合法性。可知 $(Y_h,X_h)$ 是医疗机构的部分公私钥，$(Y_d,X_d)$ 是医生的部分公私钥，$(Y_p,X_p)$ 是患者的部分公私钥。

### 3.4　加密存储医疗数据

医生结束治疗时上传患者医疗数据的密文在 IPFS 中，减少过度占用区块链的空间。具体如下。

1) 医生使用自己的私钥计算共享密钥 $k_{d,p} = x_dy_p$，通过安全信道发送共享密钥 $k_{d,p}$ 给患者 $\text{ID}_p$。随后医生用共享密钥 $k_{d,p}$ 计算对称密钥 $K_A = F(k_{d,p})$。

2) 医生通过高级加密标准 AES 的加密算法和 $K_A$ 计算得到医疗数据 $m$ 的密文 $c_m = E_{K_A}(m)$。

3) 医生上传 $c_m$ 至 IPFS 上存储，然后，IPFS 返回存储地址 $u$。医生使用 $K_A$ 计算地址密文 $c_u = E_{K_A}(u)$。

4) 医生将患者身份信息 $\text{ID}_p$ 和存储地址密文 $c_u$ 上传到区块链上。

### 3.5　签密

请求医疗机构的区块链发起跨链请求。患者的医疗数据在目的区块链审核节点中通过审核之后，智能合约执行如下操作。

1) 智能合约任意选择 $v \in \mathbb{Z}_q^*$，计算 $V = vG$，$W = v(y_h' + H_1(y_h',\text{ID}_h')y_{\text{pub}} + Y_h')$，$C = c_u \oplus H_2(V,W)$，

其中，$V,W$表示计算过程中的中间参数，$y_h'$表示请求医疗机构的公钥，$\mathrm{ID}_h'$表示请求医疗机构的身份信息，$Y_h'$表示请求医疗机构的部分公钥。

2) 智能合约发送$(c_u,V)$给医疗机构的管理者请求签名。管理者计算$I=H_3(c_u,V)$，选取$z\in\mathbb{Z}_q^*$，计算$Z_1=zG$，$Z_2=(x_h+X_h)I+z \bmod q$，返回$(Z_1,Z_2)$给智能合约，其中，$I,Z_1$表示计算过程中的中间参数，$Z_2$表示管理者对地址密文$c_u$的签名。

3) 智能合约输出最终的密文$\sigma=(V,C,Z_1,Z_2)$给跨链网关。

### 3.6　解签密

请求区块链的智能合约收到跨链网关的密文$\sigma$时，操作如下。

1) 智能合约发送密文$V$给医疗机构管理者，管理者计算$W=(x_h'+X_h')V$，将$W$发给智能合约，智能合约计算$c_u=C\oplus H_2(V,W)$。

2) 智能合约得到$c_u$，随后验证等式$Z_2G=H_3(c_u,V)(y_h+H_1(y_h,\mathrm{ID}_h)y_{\mathrm{pub}}+Y_h)+Z_1$是否成立。验证过程为

$$Z_2G=((x_h+X_h)I+z)G=H_3(c_u,V)(y_h+H_1(y_h,\mathrm{ID}_h)y_{\mathrm{pub}}+Y_h)+Z_1 \quad (1)$$

由于使用签密者的公钥即可验证，故能够确定签密者身份和地址密文的正确性。

### 3.7　解密医疗数据

跨链请求的源区块链智能合约在通过验证后，发送来自IPFS的地址密文$c_u$给医生。医生向患者请求共享密钥$k_{d,p}$，生成对称密钥$K_A$解密得到地址$u$，使用$u$从IPFS中下载医疗数据密文$c_m$。通过AES的解密算法$D_{K_A}(c_m)$计算得到明文$m$，然后使用明文$m$即可对患者进行治疗。

## 4　跨链数据共享过程

跨链数据共享过程如图2所示，具体如下。

1) 区块链$A$中节点发起跨链请求时，智能合约生成跨链请求记录在区块链$A$上，将请求发给跨链网关$A$，跨链网关$A$将请求发给中继链。

2) 中继链收到区块链$A$的跨链请求后，验证跨链请求。如果验证通过，将其发给跨链网关$B$，跨链网关$B$将请求转发给区块链$B$。

3) 区块链$B$的智能合约收到区块链$A$的跨链请求时，交由审核节点根据患者的信息分析。为了使跨链医疗数据共享效果达到最理想情况，医生上传数据至区块链时先使用本文方案分类处理医疗数据，根据患者的病情进行标记（特殊标记和普通标记），将标记嵌入到患者身份中并上传区块链。如果病人的病情在原医院无法治疗，就需要转院处理；患者离开原医疗机构时医生向智能合约提出申

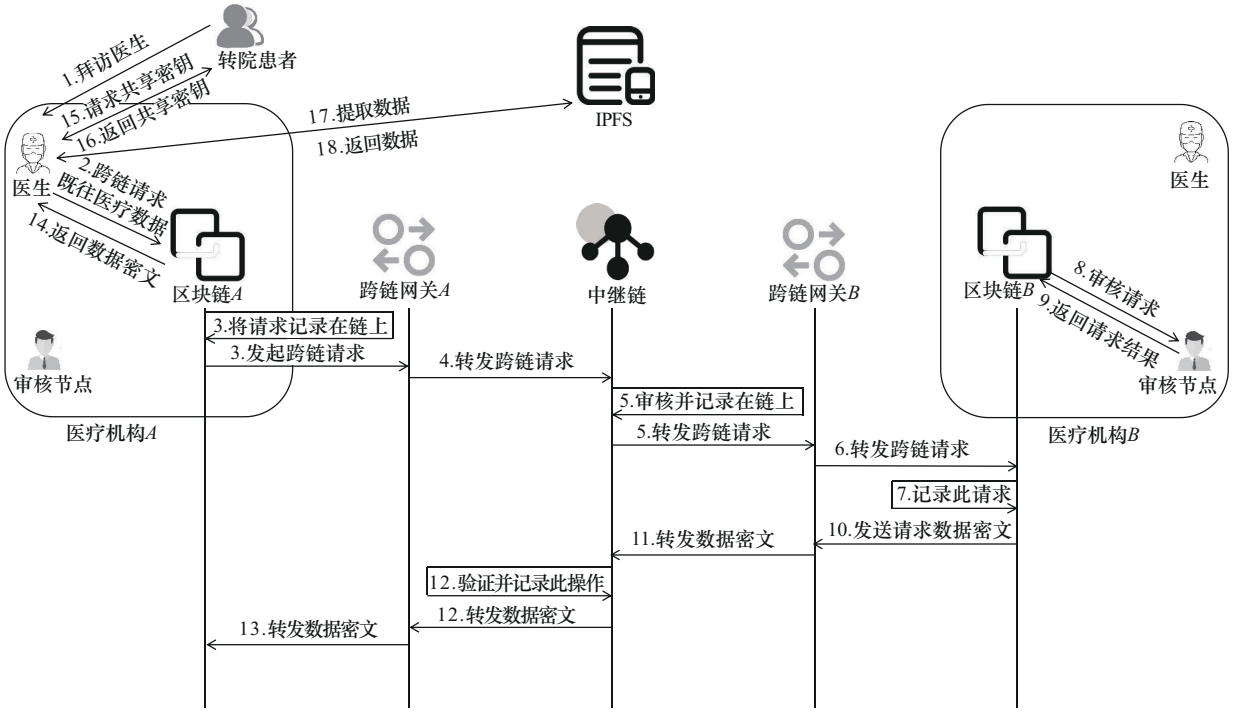


图2　基于本文方案的跨链数据共享过程

请，智能合约对请求信息进行签密，转发至待请求的消息队列中，等待跨链数据请求。目标区块链的响应过程：区块链$B$的智能合约收到跨链请求时，审核节点首先根据患者身份查询是否为等待请求信息。如果是，从待请求队列中转发此信息至跨链网关，然后记录在区块链上；否则，审核节点根据请求患者身份判断患者的类型：对于特殊患者，审核节点得到患者确认后，将此结果记录在区块链上，然后加入转发队列，等待跨链网关转发；对于普通患者，在区块链上记录此操作并加入转发队列。

4) 中继链审核跨链网关$B$转发的数据，如果核实通过，将此操作记录在中继链上，随后转发给跨链网关$A$。

5) 区块链$A$收到网关$A$转发的数据后，利用智能合约进行解密，发送解密后的信息给患者目前的主治医生。

## 5　医疗数据的删除或修改

由于某些患者身份特殊，需要删除在原机构的医疗数据；某些患者病情发生重大变化还要更新医疗数据。为了解决上述问题，本文方案在智能合约上部署了删除或修改患者医疗数据的操作。加密医疗数据记录在IPFS中，故删除或修改记录在IPFS中的医疗数据是可实现的。具体介绍如下。

1) 患者$\mathrm{ID}_p$向系统管理中心申请删除或修改。患者$\mathrm{ID}_p$在申请消息$R_p$中阐明原因。患者$ID_p$选择随机数$t\in\mathbb{Z}_q^*$，计算$T_1=tG$，$T_2=ty_{\mathrm{pub}}$，$C_R=R_p\oplus H_4(T_1,T_2)$，$I_R=H_5(R_p,T_1)$。接着患者$\mathrm{ID}_p$计算签名$Z_R=(x_p+X_P)I_R+t \bmod q$。患者$ID_p$向系统管理中心发送申请理由的密文$\sigma_R=(T_1,C_R,Z_R)$。

2) 系统管理中心工作人员在收到患者$ID_p$的密文$\sigma_R$时，使用系统管理中心的私钥计算得到$T_2'=sT_1(T_2'=sT_1=stG=ty_{\mathrm{pub}}=T_2)$，$R_p'=C_R\oplus H_4(T_1,T_2')$。如果下列等式成立：$Z_RG=H_5(R_p',T_1)(y_p+H_1(y_p,\mathrm{ID}_p)y_{\mathrm{pub}}+Y_P)+T_1$，工作人员接受患者申请；否则，工作人员拒绝患者申请。验证过程如下

$$\begin{aligned}&Z_RG=[(x_p+X_p)I_R+t]G=\\&H_5(R_p',T_1)(x_p+\varphi_p s+X_p)G+T_1=\\&H_5(R_p',T_1)(y_p+H_1(y_p,\mathrm{ID}_p)y_{\mathrm{pub}}+Y_p)+T_1\end{aligned}\tag{2}$$

如果$R_p'=R_p$，即可验证成功。

3) 工作人员审核通过的情况下生成同意删除或修改操作的签密消息，与$R_p$同长的$R_{s,p}$表示管理中心同意删除或修改的标识信息。工作人员计算$N=nG(n\in\mathbb{Z}_q^*)$,$M=n(y_h+H_1(y_h,\mathrm{ID}_h)y_{\mathrm{pub}}+Y_h)$,$C_{s,p}=(R_{s,p},R_p)\oplus H_6(N,M)$，$I_{s,p}=H_5(R_{s,p},N)$，$Z_{s,p}=sI_{s,p}+n \bmod q$。工作人员输出签密信息$\sigma_{s,p}=(N,C_{s,p},Z_{s,p})$和患者签名信息$(T_1,Z_R)$给医疗数据存储地址密文所在区块链的跨链网关。

4) 跨链网关转发收到的系统管理中心的签密信息$\sigma_{s,p}$给区块链智能合约。具体如下：智能合约发送$\sigma_{s,p}$中的$N$给医疗机构管理者，管理者使用自己的私钥计算$M'=(x_h+X_h)N$，随后通过安全信道发送$M'$给智能合约。智能合约计算得到$(R_{s,p}',R_p')=C_{s,p}\oplus H_6(N,M')$。验证过程如下：$M'=(x_h+X_h)N=(x_h+\varphi_h s+d_h)nG=n(y_h+H_1(y_h,\mathrm{ID}_h)y_{\mathrm{pub}}+Y_h=M$。然后验证下列两个公式是否同时成立：$Z_{s,p}G=H_5(R_{s,p}',N)y_{\mathrm{pub}}+N$，$Z_RG=H_5(R_p',T_1)(y_p+H_1(y_p,\mathrm{ID}_p)y_{\mathrm{pub}}+Y_p)+T_1$。由于$Z_{s,p}G=(sI_{s,p}+n)G=H_5(R_{s,p}',N)y_{\mathrm{pub}}+N$，如果$R_{s,p}'=R_{s,p}$，验证成功。$Z_RG$的验证与2)中的验证相同。如果上述两等式都成立，智能合约根据$R_{s,p}$中操作标识向IPFS发送操作指令。对于删除指令，IPFS执行删除操作，智能合约记录此操作在区块链上。对于修改指令，IPFS先删除原医疗数据，智能合约向患者发出重新上传的指令，患者和主治医生上传重新加密的医疗数据到IPFS中，得到新存储地址，地址密文上传区块链的操作与3.4节相同；否则，智能合约拒绝接受管理中心的命令。

本文原始医疗数据的密文存储在IPFS中，区块链上存储IPFS返回的地址密文，删除或修改操作在IPFS中进行，只在区块链上增加一条交易信息，区块链其他节点只备份新交易信息；整个区块链只是一次正常操作，不会增加任何额外的开销。如果其他节点使用原始地址向IPFS请求密文，IPFS不会导向任何有关信息，如果其他节点无法收到IPFS返回的地址密文，说明此医疗数据已被删除或修改，需要重新在区块链中搜索有关信息。

## 6　安全性证明

**定理1**　如果敌手$A_1$能攻破本文方案的IND-CCA2-I安全性，则必定存在挑战算法$\Gamma$能够解决ECCDH问题。

**证明**　假设$\Gamma$收到ECCDH问题的随机实例$(G,aG,bG)$。$\Gamma$试图利用$A_1$计算$\omega=abG$，$a,b\in\mathbb{Z}_q^*$

对于$(\Gamma,A_1)$是未知的。游戏中$A_1$充当$\Gamma$的子程序。$\Gamma$维护初始为空的列表$J_1$、$J_2$、$J_3$、$J_4$、$J_5$、$J_6$、$J_7$、$J_{\mathrm{PK}}$分别用来记录过程中$H_i(i=1,2,3,4,5,6)$预言机、$F$预言机及公钥预言机的询问-应答值。$\Gamma$选取整数$\tau\in\{1,2,\cdots,J_{PK}\}$，确定挑战身份$\mathrm{ID}_\tau$，$(\tau,\mathrm{ID}_\tau)$对于$A_1$是未知的，$\delta$是$\mathrm{ID}_i=\mathrm{ID}_\tau$的概率。$\Gamma$输出通过初始化算法得到的系统参数$\pi(y_{\mathrm{pub}}=aG)$给$A_1$。在阶段1中（即敌手初始询问阶段），$A_1$向$\Gamma$提交多项式有界次适应性询问。

公钥询问：$A_1$询问身份$\mathrm{ID}_i$的公钥$y_i$，如果$J_{PK}$中有匹配公钥，$\Gamma$输出$y_i$给$A_1$；否则，$\Gamma$选取$x_i\in\mathbb{Z}_q^*$，输出$y_i\leftarrow x_iG$给$A_1$，添加$(\mathrm{ID}_i,x_i,y_i)$到$J_{PK}$中。

私钥询问：$A_1$询问$ID_i$的私钥$x_i$，如果$\mathrm{ID}_i=\mathrm{ID}_\tau$，$\Gamma$终止游戏；否则，$\Gamma$查询$J_{PK}$并输出私钥$x_i$给$A_1$。

$H_1$询问：$A_1$提交$H_1$询问。如果$J_1$中有匹配元组，$\Gamma$输出$\varphi_i$给$A_1$；否则，$\Gamma$输出任意选取的$\varphi_i\in\mathbb{Z}_q^*$给$A_1$，添加$(\mathrm{ID}_i,y_i,\varphi_i,-,-)$到$J_1$中。

部分公钥询问：$A_1$询问$\mathrm{ID}_i$的部分公钥$Y_i$。若$\mathrm{ID}_i=\mathrm{ID}_\tau$，$\Gamma$调用$H_1$预言机得到$\varphi_i$，输出$Y_i\leftarrow aG-\varphi_iaG$给$A_1$。$\Gamma$然后添加元组$(\mathrm{ID}_i,y_i,\varphi_i,-,Y_i)$到$J_1$中。否则，$\Gamma$调用$H_1$预言机得到$\varphi_i$，选取$d_i\in\mathbb{Z}_q^*$，输出$Y_i\leftarrow d_iG-\varphi_iaG$给$A_1$，添加$(\mathrm{ID}_i,y_i,\varphi_i,d_i,Y_i)$到$J_1$中。

部分私钥询问：$A_1$询问$\mathrm{ID}_i$的部分私钥$X_i$。若$\mathrm{ID}_i=\mathrm{ID}_\tau$，$\Gamma$终止游戏；否则，$\Gamma$从$J_1$中选择$\mathrm{ID}_i$对应的$d_i$给$A_1$。$A_1$通过$X_iG=\varphi_iy_{\mathrm{pub}}+Y_i$验证$X_i$的有效性。

替换公钥：$A_1$随机选取$y_i,Y_i\in\mathbb{G}$替换$\mathrm{ID}_i$的整体公钥$(y_i,Y_i)$。如果$\mathrm{ID}_i=\mathrm{ID}_\tau$，$\Gamma$终止游戏；否则，$\Gamma$利用$(\mathrm{ID}_i,-,y_i)$替换$J_{PK}$中对应的$(\mathrm{ID}_i,x_i,y_i)$，使用$(\mathrm{ID}_i,y_i,-,-,Y_i)$替换$J_1$中对应的元组$(\mathrm{ID}_i,y_i,\varphi_i,d_i,Y_i)$。

$H_2$询问：$A_1$提交$H_2$询问。如果$J_2$中有匹配的元组，$\Gamma$输出$\theta$给$A_1$；否则，$\Gamma$输出任意选取的$\theta\in\{0,1\}^{L_2}$给$A_1$，添加$(V,M,\theta)$到$J_2$中。

$H_3$询问：$A_1$提交$H_3$询问。如果$J_3$中有匹配的元组，$\Gamma$输出$\vartheta$给$A_1$；否则，$\Gamma$输出任意选取的$\vartheta\in\mathbb{Z}_q^*$给$A_1$，添加$(c_u,V,\vartheta)$到$J_3$中。

$H_4$询问：$A_1$提交$H_4$询问。如果$J_4$中有匹配的元组，$\Gamma$输出$\theta_1$给$A_1$；否则，$\Gamma$输出任意选取的$\theta_1\in\{0,1\}^{L_R}$给$A_1$，添加$(T_1,T_2,\theta_1)$到$J_4$中。

$H_5$询问：$A_1$提交$H_5$询问。如果$J_4$中有匹配的元组，$\Gamma$输出$\theta_2$给$A_1$；否则，$\Gamma$输出任意选取的$\theta_2\in\mathbb{Z}_q^*$给$A_1$，添加$(R_P,T_1,\theta_2)$到$J_5$中。

$H_6$询问：$A_1$提交$H_6$询问。如果$J_6$中有匹配的元组，$\Gamma$输出$\theta_3$给$A_1$；否则，$\Gamma$输出任意选取的$\theta_3\in\{0,1\}^{L_R+L_R}$给$A_1$，添加$(N,M,\theta_3)$到$J_6$中。

$F$询问：$A_1$提交$F$询问。如果$J_7$中有匹配的元组，$\Gamma$输出$\theta_4$给$A_1$；否则，$\Gamma$输出任意选取的$\theta_4\in\{0,1\}^{L_3}$给$A_1$，添加$(k_{d,p},\theta_4)$到$J_7$中。

签密询问：$A_1$询问$(c_u,\mathrm{ID}_h,\mathrm{ID}_h')$的签密询问。如果$\mathrm{ID}_h\neq\mathrm{ID}_\tau$，$\Gamma$通过签密算法输出密文$\sigma$给$A_1$。如果$\mathrm{ID}_h=\mathrm{ID}_\tau$，$\Gamma$任选$v,z\in\mathbb{Z}_q^*$，计算$V=vG,W=v(y_h'+H_1(y_h',\mathrm{ID}_h')y_{\mathrm{pub}}+Y_h')$，$C=c_u\oplus H_2(V,W)$，$\Gamma$添加$(V,W,\theta\leftarrow H_2(V,W))$到$J_2$中。$\Gamma$计算$I=H_3(c_u,V)$，$Z_1=zG$，添加$(c_u,V,\vartheta\leftarrow H_3(c_u,V))$到$J_3$中，得到满足$Z_2G=H_3(c_u,V)(y_h+H_1(y_h,\mathrm{ID}_h)y_{\mathrm{pub}}+Y_h)+Z_1$的$Z_2$，输出密文$\sigma=(V,C,Z_1,Z_2)$给$A_1$。

解签密询问：$A_1$提交解签密询问。如果$\mathrm{ID}_h'\neq\mathrm{ID}_\tau$，$\Gamma$通过解签密算法输出$c_u$或$\perp$给$A_1$。否则，$\Gamma$在$J_2$中寻找针对$x_i$不同的元组$(V,M,\theta)$，使得$A_1$询问$(V,y_{\mathrm{pub}},\omega)$时，$O_{\mathrm{ECCDH}}$返回1。

如果有这种情况，$\Gamma$通过$A_1$或$J_{PK}$得到$x_h'$，计算$\gamma=x_h'V$，$W=\gamma+\omega$，$c_u=C\oplus\theta$。如果$Z_2G=H_3(c_u,V)(y_h+H_1(y_h,\mathrm{ID}_h)y_{\mathrm{pub}}+Y_h)+Z_1$，$\Gamma$输出$c_u$；否则，$\Gamma$输出$\perp$给$A_1$。

$A_1$提交等长消息$(c_{u0},c_{u1})$和身份$(\mathrm{ID}_h^*,\mathrm{ID}_h^{*\prime})$给$\Gamma$。挑战前$A_1$不能询问$\mathrm{ID}_h^{*\prime}$的私钥。如果$\mathrm{ID}_h^{*\prime}\neq\mathrm{ID}_\tau$，$\Gamma$在终止游戏；否则，$\Gamma$任选$\rho\in\{0,1\}$，计算$V^*=bG$，$W^*=x_h^{*\prime}V^*+\omega^*$，$C^*=c_{u,\rho}\oplus H_2(V^*,W^*)$，$(c_{u\rho},V^*,\vartheta^*\leftarrow H_3(c_{u\rho},V^*))$记录到$J_3$中，可以得到满足等式$Z_2^*G=H_3(c_u,V^*)(y_h^*+H_1(y_h^*,\mathrm{ID}_h^*)y_{\mathrm{pub}}+Y_h^*)+Z_1^*$的$Z_2^*$，输出挑战密文$\sigma^*=(V^*,C^*,Z_1{}^*,Z_2{}^*)$给$A_1$。

$A_1$在阶段2（即上述挑战结束后，敌手根据挑战的结果，继续询问的阶段）再次提交像阶段1那样的询问。$A_1$不能询问$\mathrm{ID}_h^{*\prime}$的完整私钥，也不能提交$\sigma^*$给解签密预言机。最后，$\Gamma$输出ECCDH问题实例的解答$\omega^*=X_h^{*\prime}V^*=abG$。

假设$\varepsilon$是$A_1$攻破IND-CCA2-I安全性的优势，e是自然对数底，$J_2$是$A_1$询问$H_2$预言机的次数，$J_{sk}$

是询问私钥的次数，$J_{sk'}$是询问部分私钥的次数，$J_r$是替换公钥的次数。$\Gamma$解决ECCDH问题的概率至少是$\frac{\varepsilon}{\mathrm{e}J_2(J_{sk}+J_{sk'}+J_r)}$[14]。证毕。

**定理2**　如果敌手$A_2$能攻破本文方案的IND-CCA2-II安全性，则必定存在挑战算法$\Gamma$能够解决ECCDH问题。

**证明**　假设$\Gamma$收到ECCDH问题的一个随机实例$(G,aG,bG)$。$\Gamma$试图确定$\omega=abG\in\mathbb{G}$，$a,b\in\mathbb{Z}_q^*$对于$(\Gamma,A_2)$是未知的。$\Gamma$输出通过设置算法得到的全局参数$\pi(y_{\mathrm{pub}}=sG)$，输出$\pi$给$A_2$。在阶段1中，$A_2$向$\Gamma$提交下面适应性询问。哈希预言机询问与定理1的阶段1相同，故略去。

公钥询问：$A_2$询问$\mathrm{ID}_i$的公钥$y_i$。如果$\mathrm{ID}_i=\mathrm{ID}_\tau$，$\Gamma$输出公钥$y_i\leftarrow aG$给$A_2$，添加$(\mathrm{ID}_i,-,y_i)$到$J_{\mathrm{PK}}$中。否则，$\Gamma$输出$y_i\leftarrow x_iG$（$x_i\in\mathbb{Z}_q^*$）给$A_2$，添加$(\mathrm{ID}_i,x_i,y_i)$到$J_{PK}$中。

私钥询问：$A_2$询问$\mathrm{ID}_i$的私钥$x_i$，如果$\mathrm{ID}_i=\mathrm{ID}_\tau$，$\Gamma$终止游戏；否则，$\Gamma$查询$J_{PK}$并输出私钥$x_i$给$A_2$。

部分公钥询问：$A_2$询问$\mathrm{ID}_i$的部分公钥$Y_i$。$J_1$中存在部分公钥，$\Gamma$输出$Y_i$给$A_2$；否则，$\Gamma$任意选取$d_i\in\mathbb{Z}_q^*$，输出$Y_i\leftarrow d_iG$给$A_2$，添加$(\mathrm{ID}_i,y_i,\varphi_i,d_i,Y_i,-)$到$J_1$中。

部分私钥询问：$A_2$询问$\mathrm{ID}_i$的部分私钥$X_i$。$J_1$中存在部分私钥，$\Gamma$输出$X_i$给$A_2$；否则，$\Gamma$输出$X_i\leftarrow\varphi_i s+d_i$给$A_2$，添加$(\mathrm{ID}_i,y_i,\varphi_i,d_i,-,X_i)$到$J_1$中。$A_2$通过$X_iG=\varphi_i y_{\mathrm{pub}}+Y_i$验证$X_i$的有效性。

签密询问：$A_2$提交$(c_u,\mathrm{ID}_h,\mathrm{ID}_h')$的签密询问。如果$\mathrm{ID}_h\neq\mathrm{ID}_\tau$，$\Gamma$通过签密算法输出密文$\sigma$给$A_2$。否则，$\Gamma$随机选取$v,z\in\mathbb{Z}_q^*$，计算$V=vG,W=v(y_h'+H_1(y_h',\mathrm{ID}_h')y_{\mathrm{pub}}+Y_h')$，$C=c_u\oplus H_2(V,W)$，添加$(V,W,\theta\leftarrow H_2(V,W))$到$J_2$中。$\Gamma$继续计算$I=H_3(c_u,V)$，$Z_1=zG$。$\Gamma$添加$(c_u,V,\vartheta\leftarrow H_3(c_u,V))$到$J_3$中，得到满足$Z_2G=H_3(c_u,V)(y_h+H_1(y_h,\mathrm{ID}_h)y_{\mathrm{pub}}+Y_h)+Z_1$的$Z_2$，输出密文$\sigma=(V,C,Z_1,Z_2)$给$A_2$。

解签密询问：$A_2$提交解签密询问。如果$\mathrm{ID}_h'\neq\mathrm{ID}_\tau$，$\Gamma$通过解签密算法输出$c_u$或$\perp$给$A_2$。否则，$\Gamma$在$J_2$中寻找针对$X_i'$不同元组$(V,M,\theta)$，使$A_2$询问$(V,y_i,\omega)$时$O_{\mathrm{ECCDH}}$返回1。如果有此情况，$\Gamma$计算$\gamma=X_h'V$，$W=\gamma+\omega$，$c_u=C\oplus\theta$。若$Z_2G=H_3(c_u,V)(y_h+H_1(y_h,\mathrm{ID}_h)y_{\mathrm{pub}}+Y_h)+Z_1$，$\Gamma$输出$c_u$给$A_2$；否则，$\Gamma$输出$\perp$给$A_2$。

$A_2$提交等长消息$(c_{u0},c_{u1})$和身份$(\mathrm{ID}_h^*,\mathrm{ID}_h^{*\prime})$给$\Gamma$。挑战前，$A_2$不能询问$ID_h^{*\prime}$的私钥。如果$\mathrm{ID}_h^{*\prime}\neq\mathrm{ID}_\tau$，$\Gamma$终止游戏；否则，$\Gamma$随机选取$\rho\in\{0,1\}$，计算$V^*=bG$，$W^*=X_h^{*\prime}V^*+\omega^*$，$C^*=c_{u\rho}\oplus H_2(V^*,W^*)$，$(c_{u\rho},V^*,\vartheta^*\leftarrow H_3(c_{u\rho},V^*))$记录在$J_3$中，得到满足$Z_2^*G=H_3(c_u,V^*)(y_h^*+H_1(y_h^*,\mathrm{ID}_h^*)y_{\mathrm{pub}}+Y_h^*)+Z_1^*$的$Z_2^*$，输出挑战密文$\sigma^*=(V^*,C^*,Z_1{}^*,Z_2{}^*)$给$A_2$。

$A_2$在阶段2再次提交像阶段1那样的询问。$A_2$不能提取$\mathrm{ID}_h^{*\prime}$的私钥，也不能提交$\sigma^*$给解签密预言机。$\Gamma$输出ECCDH问题实例的解答：$\omega^*=x_h^{*\prime}V^*=abG$。$\Gamma$解决ECCDH问题的概率至少是$\frac{\varepsilon}{\mathrm{e}J_2J_{sk}}$[14]。证毕。

**定理3**　如果敌手$A_1$能攻破本文方案的UF-CMA-I安全性，则存在挑战算法$\Gamma$能解决ECDL问题。

**证明**　假设令$\Gamma$收到ECDL困难问题的随机实例$(G,aG)$。$\Gamma$试图得到$a\in\mathbb{Z}_q^*$。$\Gamma$输出通过初始化算法得到的系统参数$\pi(y_{\mathrm{pub}}=aG)$给$A_1$。$A_1$向$\Gamma$发出与定理1中阶段1相同的询问。询问结束时，$A_1$输出$(\mathrm{ID}_h^*,\mathrm{ID}_h^{*\prime},\sigma^*\leftarrow(V^*,C^*,Z_1{}^*,Z_2{}^*))$给$\Gamma$。询问中$A_1$不能提取$\mathrm{ID}_h^{*\prime}$的完整私钥，$\sigma^*$不应该是任何签密预言机的应答。如果$\mathrm{ID}_h^{*\prime}\neq\mathrm{ID}_\tau$，$\Gamma$终止游戏；否则，$\Gamma$通过调用相应预言机伪造输出另一密文$(\mathrm{ID}_h^{**},\mathrm{ID}_h^{**\prime},\sigma^{**}\leftarrow(V^{**},C^{**},Z_1{}^{**},Z_2{}^{**}))$。$\Gamma$使用分叉引理得到ECDL困难问题实例的解答。

$$\begin{cases} Z_2^*G=I^*(y_h^*+H_1(y_h^*,\mathrm{ID}_h^*)aG+Y_h^*)+Z_1^* \\ Z_2^{**}G=I^{**}(y_h^{**}+H_1(y_h^{**},\mathrm{ID}_h^{**})aG+Y_h^{**})+Z_1^{**} \end{cases} \tag{3}$$

$$a=\frac{Z_2^*-Z_2^{**}-I^*(x_h^*+d_h^*)+I^{**}(x_h^{**}+d_h^{**})-z^*+z^{**}}{I^*H_1(y_h^*,\mathrm{ID}_h^*)-I^{**}H_1(y_h^{**},\mathrm{ID}_h^{**})} \tag{4}$$

根据定理1，$\Gamma$解决ECDL问题的概率至少是$\frac{\varepsilon}{\mathrm{e}(J_{sk}+J_{sk'}+J_r)}$。证毕。

**定理4**　如果敌手$A_2$能攻破本文方案的UF-CMA-II安全性，则存在挑战算法$\Gamma$能解决ECDL问题。

**证明**　假设令$\Gamma$收到一个ECDL困难问题的随机实例$(G,aG)$。$\Gamma$试图确定$a\in\mathbb{Z}_q^*$。$\Gamma$输出通过初始化算法得到的系统参数$\pi(y_{\mathrm{pub}}=sG)$给$A_2$。$A_2$向

$\Gamma$发出与定理1中阶段1相同的询问。

询问结束时，$A_2$输出一个伪造密文$(\mathrm{ID}_h^*,\mathrm{ID}_h^{*\prime},\sigma^* \leftarrow (V^*,C^*,Z_1{}^*,Z_2{}^*))$给$\Gamma$。询问中$A_2$不能提取$\mathrm{ID}_h^{*\prime}$的完整私钥，$\sigma^*$不该是任何签密预言机的应答。如果$\mathrm{ID}_h^{*\prime} \neq \mathrm{ID}_\tau$，$\Gamma$终止游戏。否则，$\Gamma$伪造输出另一密文$(\mathrm{ID}_h^{**},\mathrm{ID}_h^{**\prime},\sigma^{**} \leftarrow (V^{**},C^{**},Z_1{}^{**},Z_2{}^{**}))$。$\Gamma$使用分叉引理得到ECDL问题实例的解答

$$\begin{cases} Z_2^* G = I^*(aG + H_1(y_h^*,\mathrm{ID}_h^*)y_{\mathrm{pub}} + Y_h^*) + Z_1^* \\ Z_2^{**} G = I^{**}(aG + H_1(y_h^{**},\mathrm{ID}_h^{**})y_{\mathrm{pub}} + Y_h^{**}) + Z_1^{**} \end{cases} \tag{5}$$

$$a = \frac{Z_2^* - Z_2^{**} - I^*(\varphi_h^* s + d_h^*) + I^{**}(\varphi_h^{**} s + d_h^{**}) - z^* + z^{**}}{I^* - I^{**}} \tag{6}$$

依据定理2，$\Gamma$解决ECDL问题的概率至少$\frac{\varepsilon}{\mathrm{e}J_{sk}}$。证毕。

## 7　性能分析

### 7.1　特征和安全性对比

表1对各个方案的特征进行对比。可以看出，只有本文方案支持医疗数据在传输中的分层处理和医疗数据的更改或删除，这使跨链技术的应用价值得到极大提高。本文对比各个方案中的双花攻击、重放攻击、仿冒攻击、女巫攻击和日蚀攻击等安全指标，如表2所示。双花攻击：攻击者在一条链上完成交易后，试图在另一条链上撤回或重复这笔资产，导致资产在不同链上重复使用。重放攻击：攻击者拦截并复制合法的交易数据，然后在另一条链上重复发送，实现欺诈性的交易操作。仿冒攻击：攻击者通过冒充参与交易的某方窃取资产或破坏交易完整性，在跨链交易中进行未经授权的操作。女巫攻击：攻击者通过创建多个伪造身份控制网络或者影响共识机制，操控交易流程、验证过程等。日蚀攻击：攻击者通过隔离受害节点与其他合法节点的区块链网络连接，使之只能与恶意节点通信。

**表1　各个方案的特征对比**

| 方案 | 机密性 | 双线性对 | 分层处理 | 更改医疗数据 |
|---|---|---|---|---|
| 文献[7] | √ | √ | × | × |
| 文献[10] | √ | √ | × | × |
| 文献[13] | √ | √ | × | × |
| 本文方案 | √ | × | √ | √ |

**表2　各个方案安全性对比**

| 方案 | 双花攻击 | 重放攻击 | 仿冒攻击 | 女巫攻击 | 日蚀攻击 |
|---|---|---|---|---|---|
| 文献[7] | √ | × | √ | √ | √ |
| 文献[10] | √ | × | √ | × | × |
| 文献[13] | √ | √ | √ | × | × |
| 本文方案 | √ | √ | √ | √ | √ |

本文方案在跨链交易时由中继链确认双方交易信息的一致性，能抵御双花攻击。中继链转发跨链信息，如果发现连续的跨链申请，拒绝转发，故能抵御重放攻击。中继链会验证跨链信息，原区块链智能合约会哈希处理跨链申请者的身份和公钥，故能抵御跨链数据申请者身份仿冒。本文方案在上传医生节点时会严格审核和验证其身份，故加入的医生节点都是诚实可信的，跨链交互时防止了女巫攻击的威胁。跨链过程中医生节点的数据交互与区块链智能合约直接进行交互，不与其他节点交互，故不存在日蚀攻击的威胁。

文献[7]、文献[10]及文献[13]部署在联盟链上，不存在跨链数据交互，还面临单链中双花攻击和重放攻击。文献[7]能够给系统用户颁发数字证书，验证系统的用户身份，所以能抵御仿冒攻击、女巫攻击、日蚀攻击；没有对用户下载医疗数据进行限制，攻击者可利用合法请求多次下载，造成区块链计算负担，故不能抵御重放攻击。文献[10]使用基于属性的身份访问控制，能验证系统访问者的身份，但未对系统用户身份进行验证，故存在女巫攻击和日蚀攻击；也未对医疗数据访问次数进行控制，故存在重放攻击。文献[13]未对系统用户的身份进行验证，所以存在女巫攻击和日蚀攻击。

### 7.2　计算开销

实验平台：Windows 10操作系统，2.40 GHz Intel(R) Core(TM) i5-9300H，内存为16 GB。通过VC++ 6.0软件调用PBC库，表3列出通过多次实验得到主要密码操作运行的平均计算时间。

**表3　主要密码操作运行的平均计算时间**

| 操作类型 | 平均计算时间/ms |
|---|---|
| 椭圆曲线加法运算$T_{\mathrm{A}}$ | 0.04 |
| 椭圆曲线标量乘法运算$T_{\mathrm{M}}$ | 9.43 |
| 哈希运算$T_{\mathrm{H}}$ | 19.50 |
| 双线性运算$T_{\mathrm{P}}$ | 21.78 |
| 指数运算$T_{\mathrm{E}}$ | 1.39 |

表4统计出在数据存储阶段和数据共享阶段的计算开销，本方案基于椭圆曲线，其他方案均基于双线性配对运算。80 bit安全级别下，160 bit椭圆密码算法安全性相当于1 024 bit的双线性配对运算。本文方案在原始医疗数据加密存储时使用AES算法，提高了密文生成速度；密文存储在IPFS中，区块链上存储患者身份信息和地址密文，跨链数据交互时处理的数据更少，计算开销更低。通过中继链可确认身份，随机数使加密过程相当于安全强度高的一次一密。

**表4　数据存储阶段和数据共享阶段的计算开销**

| 方案 | 数据存储阶段 | 数据共享阶段 |
|---|---|---|
| 文献[7] | $7T_H + 2T_P + 6T_E$ | $5T_H + 5T_P + 4T_E$ |
| 文献[10] | $11T_P + 6T_E$ | $11T_P + 7T_E$ |
| 文献[13] | $7T_M + 2T_H + 2T_P$ | $T_A + 8T_M + 8T_H + 3T_P + 3T_E$ |
| 本文方案 | $T_M + T_H$ | $5T_A + 8T_M + 6T_H$ |

图3展示了数据存储和数据共享阶段的计算开销比较。从图3可以看出，本文方案总体计算开销更低。

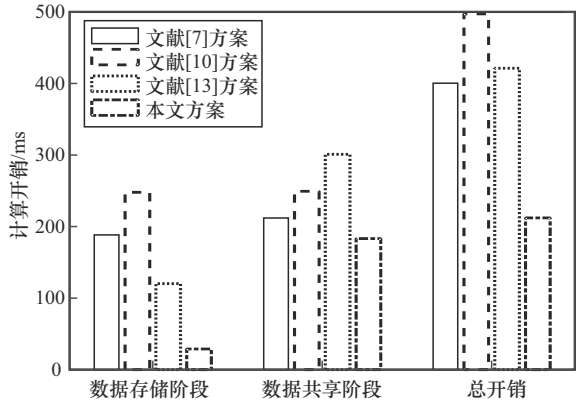


图3　数据存储和数据共享阶段的计算开销比较

### 7.3　通信开销

本文方案在同等安全级别下密钥长度更短。在数据加密存储阶段，假设本文方案使用256 bit密钥长度的AES加密原始医疗数据，密文输出长度比原始明文最多增加255 bit填充数据密文的长度。数据共享中本文方案用异或运算，不增加存储地址密文的长度。医疗数据上传区块链，跨链交互中传输的是医疗数据密文在IPFS上的存储地址密文。给定160 bit大素数生成的有限域上的椭圆曲线$E$，$G$是$E$的生成元，160 bit的$q$是$G$的阶。选择256 bit密钥长度的AES算法。本文方案中实体身份$ID_i$和医疗数据$m$都是256 bit。医疗数据存储阶段，医生生成320 bit共享密钥给患者。医生上传256 bit的数据密文$c_m$到IPFS，IPFS返回256 bit存储地址$u$。医生上传256 bit地址密文$c_u$和患者身份$ID_p$到区块链。因此，数据加密存储阶段的通信开销是320 bit + 256 bit + 256 bit + 256 bit + 256 bit=1 344 bit。

在数据共享阶段的签密中，智能合约发送256 bit的地址密文$c_u$和320 bit的参数$V$给医疗机构的管理者请求签名，管理者使用完整私钥签名得到480 bit的$(Z_1,Z_2)$给智能合约。智能合约发送密文$(V,C,Z_1,Z_2)$给跨链网关，大小是160 bit + 256 bit + 320 bit + 160 bit=896 bit。解签密中，智能合约发送320 bit的部分密文$V$给管理者，管理者计算得到320 bit的$W$给智能合约。智能合约发送地址密文$c_m$给医生。因此，数据共享阶段的通信开销是256 bit +320 bit + 480 bit + 160 bit + 256 bit + 320 bit + 160 bit + 320 bit + 320 bit + 256 bit=2 848 bit。

数据存储和数据共享阶段的通信开销比较如图4所示。从图4可以看出，本文方案总体通信开销最小。

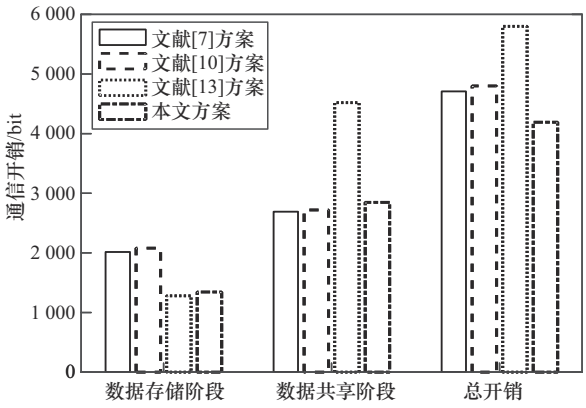


图4　数据存储和数据共享阶段的通信开销比较

## 8　结束语

区块链技术凭借其去中心化的特点可应用于医疗数据的存储，但其对外部环境高度封闭导致了医疗数据的应用性不高。本文方案能实现跨链数据的安全共享，跨链数据进行了分层处理，支持医疗数据更改或删除。伴随着物联网设备的快速发展，医疗领域不可避免会引入大量物联网设备，后续会关注区块链与医疗物联网设备深度融合中标准化接口、医疗物联网设备信息的采集和自动上传区块链等，使医疗数据的采集和上传更为简单方便。

## 参考文献：


[1] LIN G F, WANG H J, WAN J, et al. A blockchain-based fine-grained data sharing scheme for e-healthcare system[J]. Journal of Systems Architecture, 2022, 132: 102731.

[2] YU H F, BAI X P. Identity-based searchable attribute signcryption in lattice for a blockchain-based medical system[J]. Frontiers of Information Technology and Electronic Engineering, 2024, 25(3): 461-471.

[3] QIAO R, LUO X Y, ZHU S F, et al. Dynamic autonomous cross consortium chain mechanism in e-healthcare[J]. IEEE Journal of Biomedical and Health Informatics, 2020, 24(8): 2157-2168.

[4] WANG T C, WU Q S, CHEN J, et al. Health data security sharing method based on hybrid blockchain[J]. Future Generation Computer Systems, 2024, 153: 251-261.

[5] LI C Y, JIANG B H, DONG M X, et al. Efficient designated verifier signature for secure cross-chain health data sharing in BIoMT[J]. IEEE Internet of Things Journal, 2024, 11(11): 19838-19851.

[6] LI C Y, DONG M X, LI J, et al. Healthchain: secure EMRs management and trading in distributed healthcare service system[J]. IEEE Internet of Things Journal, 2021, 8(9): 7192-7202.

[7] 马雪, 潘恒, 姚中原, 等. 基于联盟链的可搜索电子病历双重授权共享方案[J]. 应用科学学报, 2023, 41(5): 881-895.
MA X, PAN H, YAO Z Y, et al. Dual authorization sharing scheme of searchable electronic medical data based on consortium blockchain[J]. Journal of Applied Sciences, 2023, 41(5): 881-895.

[8] WU G J, WANG S P, NING Z L, et al. Blockchain-enabled privacy-preserving access control for data publishing and sharing in the Internet of medical things[J]. IEEE Internet of Things Journal, 2022, 9(11): 8091-8104.

[9] MAMTA, GUPTA B B, LI K C, et al. Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system[J]. IEEE/CAA Journal of Automatica Sinica, 2021, 8 (12): 1877-1890.

[10] ZHANG L Y, ZHANG T S, WU Q, et al. Secure decentralized attribute-based sharing of personal health records with blockchain[J]. IEEE Internet of Things Journal, 2022, 9(14): 12482-12496.

[11] LIU J W, FAN Y, SUN R, et al. Blockchain-aided privacy-preserving medical data sharing scheme for E-healthcare system[J]. IEEE Internet of Things Journal, 2023, 10(24): 21377-21388.

[12] LIN C, HUANG X Y, HE D B. Efficient blockchain-based electronic medical record sharing with anti-malicious propagation[J]. IEEE Transactions on Services Computing, 2023, 16(5): 3294-3304.

[13] PENG G Y, ZHANG A Q, LIN X D. Patient-centric fine-grained access control for electronic medical record sharing with security via dual-blockchain[J]. IEEE Transactions on Network Science and Engineering, 2023, 10(6): 3908-3921.

[14] YU H F, ZHANG Q, LI L. Certificateless anti-quantum blind signcryption for e-cash[J]. Journal of Industrial Information Integration, 2024, 40: 100632.

[15] 张川, 王子豪, 梁晋文, 等. 面向跨联盟链的隐私保护数据要素交易审计方案[J]. 计算机研究与发展, 2024, 61(10): 2540-2553.
ZHANG C, WANG Z H, LIANG J W, et al. A privacy-preserving data element trading audit scheme for cross-consortium-blockchains[J]. Journal of Computer Research and Development, 2024, 61(10): 2540-2553.

[16] YU H F, MU W Z. ABE-based postquantum cross-blockchain data exchange approach for smart agriculture[J]. IEEE Transactions on Industrial Informatics, 2024, 20(10): 12083-12091.


[作者简介]


**俞惠芳**（1972– ），女，青海乐都人，博士，西安邮电大学教授、博士生导师，主要研究方向为密码学、信息安全。

**李磊**（2000– ），男，陕西咸阳人，西安邮电大学硕士生，主要研究方向为密码学、跨链数据共享。