基于区块链的电子病历数据共享方案

牛淑芬 [1] 陈俐霞 [1] 李文婷 [1] 王彩芬 [1] 杜小妮 [2]

摘 要 以区块链为数据存储平台的电子病历系统是当下研究的热点. 存储在区块链上的数据是不可变的, 这加强了数据的安全性. 提出了一个基于区块链的电子病历数据共享方案, 实现了患者和第三方数据用户在不侵犯患者隐私的前提下共享患者电子病历. 使用私有链与联盟链构造方案的系统模型, 医院服务器上存储患者的电子病历密文, 私有链上存储患者病历密文的哈希值和关键字索引, 联盟链上存储由关键字索引构成的安全索引. 同时利用可搜索加密技术实现了联盟链上对关键字的安全搜索, 运用代理重加密算法实现了第三方数据用户对患者电子病历的共享. 通过数值实验对方案进行了性能评估.

关键词 电子病历, 区块链, 代理重加密, 可搜索加密, 数据共享

引用格式 牛淑芬, 陈俐霞, 李文婷, 王彩芬, 杜小妮. 基于区块链的电子病历数据共享方案. 自动化学报, 2022, **48**(8): 2028−2038

DOI 10.16383/j.aas.c190801

Electronic Medical Record Data Sharing Scheme Based on Blockchain

NIU Shu-Fen[1] CHEN Li-Xia[1] LI Wen-Ting[1] WANG Cai-Fen[1] DU Xiao-Ni[2]

Abstract The electronic medical record system with blockchain as the data storage platform is a key research topic. The data stored in the blockchain is immutable and strengthens the security of data. This paper proposes an electronic medical record data sharing scheme based on blockchain. The scheme enables patients and third-party data users to share the patient′s electronic medical records without infringing the patient′s privacy. This paper construct system model by the private blockchain and consortium blockchain, and stores the patient′ s electronic medical record ciphertext on the hospital server. The hash of the patient′s medical record ciphertext and the keyword index are stored in the private blockchain, and the security index consisting of the keyword index is stored in the consortium blockchain. At the same time, the searchable encryption technology is used to implement secure search of keywords in the consortium blockchain, the proxy re-encryption algorithm realizes the sharing of electronic medical records of patients by third-party data users. The performance evaluation of the scheme is carried out by numerical simulation.

Key words Electronic medical record, blockchain, proxy re-encryption, searchable encryption, data sharing

Citation Niu Shu-Fen, Chen Li-Xia, Li Wen-Ting, Wang Cai-Fen, Du Xiao-Ni. Electronic medical record data sharing scheme based on blockchain. *Acta Automatica Sinica*, 2022, **48**(8): 2028−2038

随着时代的变化, 科技已渐渐融入人类生活的各个方面. 传统的医疗保健体系已然跟不上当代便捷生活的脚步, 电子病历的出现更加有效地解决了患者诊断信息的存储、查询、数据共享和医疗错误等问题[1]. 电子病历使患者拥有一个更全面的诊断信息, 在就诊时能够让医生更快捷、准确的了解患者以往病情, 并给出新的诊断结果. 文献 [2−4] 为电子病历的应用提供了切实的范例. 区块链本质上是一个去中心化的分布式存储系统, 能够为电子病历提供平台支持, 生成永久、不可逆向修改的记录[5−7]. 近年来, 鉴于区块链对电子病历的应用优势, 多位学者相继提出了针对不同问题的方案, Yue 等[8] 提出一种基于区块链的数据网关架构, 并且利用安全多方计算使第三方用户在不侵犯患者隐私的情况下对存储数据进行计算. 文献 [9] 提出了基于区块链的数据共享框架, 解决了与云中敏感信息相关的访问控制问题. 该方案是基于许可链构造的, 只允许受邀用户访问数据. 张超等[10] 构造了一个基于区块链的医疗系统, 该系统构建于联盟链之上, 通过实用拜占庭容错算法, 保证以很小的算力来实现系统安全稳定的运行, 同时能够防止医疗数据被篡改、

收稿日期 2019-11-25 录用日期 2020-05-12
Manuscript received November 25, 2019; accepted May 12, 2020
国家自然科学基金 (61562077, 61662071, 61662069, 61772022) 资助
Supported by National Natural Science Foundation of China (61562077, 61662071, 61662069, 61772022)
本文责任编委 何海波
Recommended by Associate Editor HE Hai-Bo
1. 西北师范大学计算机科学与工程学院 兰州 730070 2. 西北师范大学数学与统计学院 兰州 730070
1. College of Computer Science and Engineering, Northwest Normal University, Lanzhou 730070 2. College of Mathematics and Statistics, Northwest Normal University, Lanzhou 730070

泄露. Chen 等[11] 提出一种基于区块链共享医联体数据服务的框架, 重点突出了实施方案不依赖于任何不可信的第三方的特性, 可实现患者数据的安全存储与隐私保护. 文献 [12] 构建了一种基于区块链的保护个人隐私信息安全的共享协议, 并提出了具体的系统模型及方案. 该方案在私有链与联盟链上进行构造, 结合关键字搜索技术与联盟链实现了对患者信息的安全搜索, 同时保证了患者的数据安全和隐私保护. 区块链上电子病历的最大优势是多方数据用户都能共享患者数据, 但现有的许多文献讨论患者或者医生某一方搜索并解密病历数据. 针对这一问题, 本文提出了一种基于区块链的电子病历数据共享方案. 在方案中, 不但患者可以搜索解密自己的病历数据, 经过授权的第三方机构或个人数据用户在不能侵犯患者隐私的前提下也可以访问患者数据. 本文的创新点有以下 3 个方面:

1) 基于区块链提出了电子病历数据共享方案, 实现了第三方数据用户对患者数据的安全访问. 方案模型的构造利用了私有链与联盟链. 每家医院都拥有自己的私有链与服务器, 多个私有链一起构建联盟链. 患者病历密文存储在医院服务器, 病历密文的哈希值和关键字索引存储在医院私有链上, 而由私有链块标识、患者伪身份和关键字索引构成的安全索引则存储在联盟链上;

2) 使用可搜索加密技术实现了安全搜索. 联盟链上存储了由关键字索引所构成的安全索引. 当有患者或者数据用户需要使用电子病历数据时, 患者使用自己的私钥产生搜索陷门发送至联盟链, 联盟链上节点进行搜索;

3) 使用代理重加密技术实现了第三方数据用户对患者数据的安全访问. 经患者授权后, 联盟链上节点在搜索到患者病历的原始密文后, 对原始密文进行代理重加密, 将转换后的密文发送给第三方数据用户, 数据用户使用自己的私钥解密密文.

1 相关工作

1.1 双线性映射

定义 1. 令 G_1 和 G_2 为两个阶为素数 q 的乘法循环群, 定义一个双线性映射 $e: G_1 \times G_1 \to G_2$ 满足如下性质:

1) 双线性: 对于任意 $a, b \in Z_q^*$ 和 $x, y \in G_1$, $e(x^a, y^b) = e(x, y)^{ab}$ 成立;

2) 非退化性: 存在 $x, y \in G_1$, 使得 $e(x, y) \neq 1$;

3) 可计算性: 对于任意的 $x, y \in G_1$, 存在有效算法计算 $e(x, y)$.

1.2 可搜索加密

可搜索加密是由 Boneh 等[13] 在 2004 年提出的, 它可以对加密数据进行搜索. 在公钥密码体制下, 用户将明文消息的关键字加密后发送至服务器, 用搜索陷门搜索关键字. 在提出该密码原语之后, 对关键字搜索加密的研究陆续展开. 2008 年, Baek 等[14] 指出 Boneh 等[13] 的方案存在安全信道的问题, 通过使用服务器公钥加密搜索陷门的方法改进了方案, 并证明其安全性. 为了提高搜索的安全性, Hu 等[15] 提出了指定验证者的可搜索加密方案. 文献 [16] 将可搜索加密技术与代理重加密技术相结合, 允许被授权者从委托者的数据中搜索感兴趣的关键字. 在某些情况下需要搜索多个关键字, 文献 [17−18] 提出了带有联合字段关键字搜索的公钥加密方案. 本文提出了一种基于区块链的电子病历关键字搜索方案. 该方案将由关键字索引构成的安全索引存储在联盟链上, 实现了关键字搜索功能.

1.3 代理重加密

代理重加密是由 Blaze 等[19] 在 1998 年提出的一个新的密码原语. 代理重加密的中心思想是对密文的转换, 其参与者有委托者、代理者和受托者, 代理者能够将受托者生成的密文转换为委托者对同一消息的密文. 根据密文转换方向, 可将代理重加密分为单向和双向. 单向代理重加密能够实现受托者密文向委托者密文的转换, 双向代理重加密能够实现密文的双向转换. 近几年代理重加密仍然是密码学界中的研究热点. Fang 等[20] 提出了带关键字查询的代理重加密的概念, 并构造了具体方案. Shao 等[21] 提出了基于身份的多用户代理重加密, 并证明其安全性. Tang 等[22] 基于多线性映射构造了一个单向代理重加密方案. 刘振华等[23] 提出一个支持关键词搜索的密文策略的属性代理重加密方案, 利用属性代理重加密实现了数据转发与数据共享, 并且支持数据检索功能. 在这项工作中, 本文将代理重加密技术应用于方案的数据搜索阶段, 提出了一个基于区块链的电子病历方案, 实现了第三方数据用户对患者数据的安全访问. 当搜索到患者的原始密文后, 联盟链[24] 上节点通过使用代理重加密算法进行密文转换.

2 系统模型与安全模型

2.1 系统模型

在该系统中, 假设由多个医院组成一个联盟链,

其中每个医院都有本地服务器和和若干个客户端, 客户端是由医生进行操作的. 每家医院构建自己的私有链, 而多个私有链构建一个联盟链. 在进入系统前, 患者、医生和数据用户都需要进行注册, 生成各自的公私钥对. 其中, 患者的电子病历密文存储在医院服务器上, 电子病历密文的哈希值和关键字索引存储在医院私有链上, 而由私有链块标识、患者伪身份和关键字索引构成的安全索引则存储在联盟链上. 系统中主要包括患者、医生、数据用户、医院服务器、私有链、联盟链 6 个实体, 系统模型图如图 1 所示.

1) 患者: 患者在医院就诊时首先在医院服务器上进行注册, 注册完成后医院服务器给患者分配一个号码牌, 相当于患者的就诊卡. 患者保密该号码牌, 并在就诊时出示号码牌. 医生为患者产生电子病历和关键字, 并用患者公钥进行加密. 若患者去其他医院就诊, 当医生需要了解患者的过往病史时, 患者生成搜索陷门并上传至联盟链. 联盟链上节点运行搜索算法后, 将电子病历密文发送给患者, 患者可解密该密文.

2) 医生: 每个医院都有本地服务器和和若干个客户端, 客户端是由医生进行操作的. 当患者就诊时, 医生为患者产生伪身份、电子病历密文、关键字密文和证据, 并将电子病历密文上传至医院服务器, 将病历密文的哈希值和由关键字密文和证据构成的关键字索引上传至私有链, 产生新交易, 并广播该交易. 私有链上的其他节点负责验证该交易, 若验证通过, 则生成私有链上新的区块.

3) 数据用户: 当除了医院和患者以外的第三方机构或个人 (称为数据用户) 访问患者数据时, 需要得到患者授权. 患者生成搜索陷门并上传至联盟链, 联盟链上节点进行搜索, 当搜索到相应患者密文后, 联盟链上节点作为代理者为数据用户产生代理重加密密文. 最后, 数据用户可用自己的私钥解密密文.

4) 医院服务器: 当医生为患者治疗并生成电子病历后, 医院服务器提取私有链上的私有链块标识、患者伪身份和关键字索引来构建联盟链上新的交易, 而在联盟链中的其他节点负责验证该交易, 若验证通过, 则生成联盟链上新的区块.

5) 私有链: 医生将电子病历密文的哈希值、由关键字密文和证据构成的关键字索引上传至私有链, 产生新交易. 当收到医生构建的新交易后, 私有链上节点验证该交易. 医院服务器提取私有链上的私有链块标识、患者伪身份和关键字索引来构建联盟链上新的交易. 在数据获取阶段, 若搜索成功, 联盟链上节点提取块上安全索引, 获得私有链块标识. 而通过私有链块标识, 联盟链上节点能获取到病历密文的哈希值.

6) 联盟链: 在搜索过程中, 当收到患者发送的陷门后, 联盟链上节点运行搜索算法. 若搜索成功, 联盟链上节点提取块上安全索引, 获得私有链块标识. 通过私有链块标识, 联盟链上节点获取到病历密文哈希值并反馈给医院服务器, 医院服务器对电子病历密文的哈希值进行对比, 若一致, 则将病历密文发送给联盟链上节点, 联盟链上节点将病历密文返回给患者. 当第三方数据用户访问患者电子病历时, 联盟链上节点扮演代理者的角色生成代理重加密密钥, 对电子病历的密文进行代理重加密后并将重加密后密文发送给第三方用户.

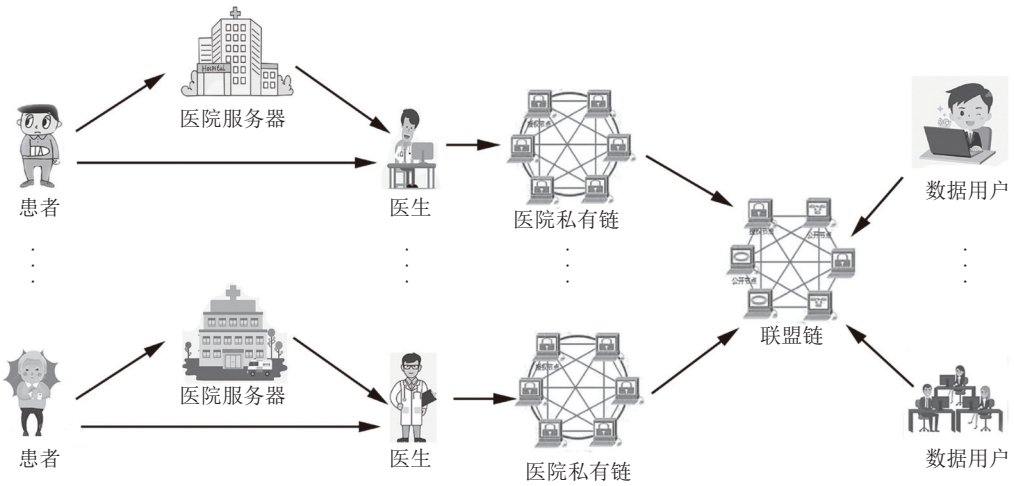

图 1 电子病历系统模型

Fig. 1 Electronic medical record system model

2.2　安全模型与设计目标

假设医院服务器与计算机客户端均为半可信, 攻击者可以窃听传输信道中的信息, 比如安全索引、电子病历密文和搜索陷门, 不允许计算机客户端与服务器串通以推断用户的真实身份. 基于以上存在的安全问题, 要实现的安全目标如下:

1) 数据安全与访问控制: 加密和签名保证了数据的机密性和完整性, 即实现了数据安全. 当医生访问数据时, 系统可以通过识别、认证和授权等机制来实现访问控制. 当数据用户访问数据时, 系统可以通过代理重加密技术来实现访问控制. 同时, 本文利用私有链和联盟链来增强数据的安全性.

2) 隐私保护: 系统通过匿名性和不可追踪性来实现患者的隐私保护. 其中患者伪身份的产生不仅实现了匿名性, 同时保护了患者的身份信息和相关的敏感隐私. 同时, 窃听者无法判断两个或多个电子病历是否来自同一患者, 保证了数据的不可链接性. 而且窃听者无法通过患者伪身份追踪患者的真实身份.

3) 安全搜索: 系统通过指定验证者来保证搜索的安全性. 在搜索过程中, 系统指定由患者生成陷门, 联盟链上节点进行搜索. 在这个过程中, 窃听者无法猜出关键字.

4) 系统可用性: 区块链的共识机制并不会泄露患者的隐私. 联盟链的一致性证明是通过验证安全索引中的关键字是否属于关键字集来实现. 在联盟链验证过程中, 窃听者并不能得到该关键字. 而私有链的一致性证明是通过验证患者是否授权医生生成病历密文来实现, 在私有链验证过程中, 窃听者无法得知患者的真实身份.

2.3　数据结构

本文在系统中使用了私有链与联盟链, 都分别存储了不同的数据, 因此具有不同的数据结构. 私有链的数据结构如表 1 所示. 它由时间戳、块头和交易组成. 块头包括: 块的 ID、块的大小和前块的哈希. 交易包括: 块产生者 (医生) 的 ID、患者伪身份、关键字索引、病历密文的哈希和块产生者 (医生) 的签名. 块产生者的签名有助于追踪医生, 时间戳显示块的生成时间, 关键字索引由关键字密文和证据构成.

联盟链的数据结构如表 2 所示. 它由时间戳、块头和交易组成. 块头包括: 块的 ID、块的大小和前块的哈希. 其中交易包括: 块产生者 (医院服务器) 的 ID、安全索引和块产生者 (医院服务器) 的签名. 医院服务器在一定时间间隔内创建新块. 期间, 医院服务器会收集私有链上块的块 ID、患者伪身份和关键字索引来构成该块的安全索引.

2.4　共识机制

本文所用的区块链系统就是一个分布式的数据库, 共识机制保证了数据的完整与同步, 即数据的一致性.

1) 私有链的一致性证明: 当患者到医院注册后, 医院服务器为其产生号码牌并分配医生. 当患者与医生交互后, 医生为患者产生电子病历密文. 为了保证患者匿名性, 医生为患者生成伪身份. 最后, 医生构建交易并广播至医院私有链. 私有链上的验证者验证患者是否授权医生生成电子病历, 即 η 与号码牌是否匹配. 若匹配, 则验证者验证通过. 若超过 2/3 的验证者验证通过, 则私有链生成新的区块.

2) 联盟链的一致性证明: 在数据加密阶段, 系统定义了一个关键字集 $W=\{w_1, w_2, \cdots, w_n\}$, 其中包含了患者有可能出现的所有症状的描述. 而本文加密的关键字都是从关键字集 W 中选取的. 在本文的系统中对联盟链的一致性证明描述为: 联盟链上的验证者验证新块中安全索引上的关键字密文是否来

表 1　私有链的数据结构

Table 1　Private chain data structure

时间戳	块头			交易				
	块标识	块大小	前块哈希	块产生者身份	患者伪身份	关键字索引	密文哈希	块产生者签名
t	ID_b	$size$	$hash$	医生 ID	ID_a	(C_{a_1}, C_{a_2})	$hash\,(C_{a_0})$	医生签名

表 2　联盟链的数据结构

Table 2　Consortium chain data structure

时间戳	块头			交易		
	块标识	块大小	前块哈希	块产生者身份	安全索引	块产生者签名
t	联盟链块 ID	$size$	$hash$	医院服务器 ID	$T_{Xa}=(ID_b, ID_a, (C_{a_1}, C_{a_2}))$	服务器签名

自关键字集 $W=\{w_1, w_2, \cdots, w_n\}$. 为了实现联盟链上的一致性证明, 系统构造了一个多项式 $f(x)$, 具体如下: 对于关键集 W, 系统计算 $H_1(w_1), H_1(w_2), \cdots, H_1(w_n)$, 并定义多项式 $f(H_1(w_i))=0, i\in(1, 2, \cdots, n)$, 即 $f(x)=(x-H_1(w_1))(x-H_1(w_2))\cdots(x-H_1(w_n))=0$. 假设存在向量 $\boldsymbol{b}=[1, b_{n-1}, \cdots, b_0]$ 使得多项式可以表示为 $f(x)=x^n+b_{n-1}x^{n-1}+\cdots+b_1x+b_0$, 转换等式为 $x^n+b_{n-1}x^{n-1}+\cdots+b_1x=-b_0$, 其中 $x=H_1(w_i), i\in(1, 2, \cdots, n)$. 若设置向量 $\boldsymbol{a}=[a_n=-b_1/b_0, \cdots, a_1=-b_1/b_0]$, 则系统可推出新多项式 $g(x)=a_nx^n+\cdots+a_1x$, 且 $g(H_1(w_i))=1,\ i\in(1, 2, \cdots, n)$. 若存在向量 $\boldsymbol{h}=\{H_1(w_1), H_1(w_2)^2, \cdots, H_1(w_n)^n\}$, 则有等式 $\boldsymbol{ah}=1$. 若数据加密过程中使用的关键字属于关键字集 $W=\{w_1, w_2, \cdots, w_n\}$, 则等式 $\boldsymbol{ah}=1$ 成立. 若超过 2/3 的验证者验证通过, 则联盟链生成新的区块.

2.5 方案模型

方案可以分为数据产生、数据存储和数据搜索三个阶段. 图 2 为数据产生与数据存储过程, 图 3 为数据搜索的过程.

假设患者 a 去医院 i 看病, 由医生 d 进行诊断. 患者 a 看病之前需要在医院 i 的服务器上进行注册.

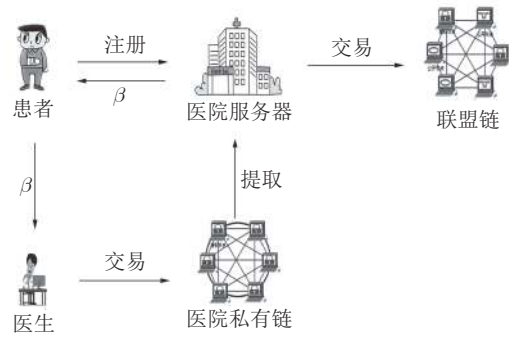

图 2 数据产生与数据存储

Fig. 2 Data generation and data storage

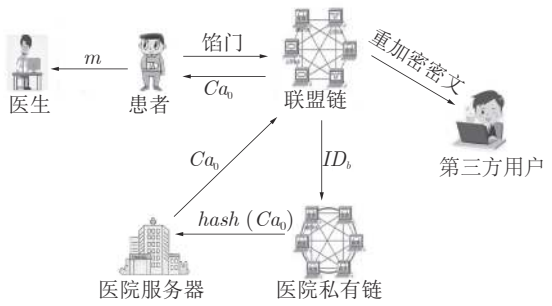

图 3 数据搜索

Fig. 3 Data search

医院的服务器为患者产生号码牌 β, 并计算 $\mu=H_1(\beta)$ 存储在系统中. 患者在见到医生后出示号码牌 β, 相当于授权给医生为自己生成电子病历 m 和关键字 w. 医生用患者的公钥 pk_a 加密 m 和 w. 输出密文 $C_a=\{C_{a_0}, C_{a_1}, C_{a_2}\}$.

C_{a_0} 为电子病历 m 的密文, C_{a_1} 为关键字 w 的密文, C_{a_2} 为联盟链上的一致性证明提供了依据. 其中, C_{a_0} 存储在医院 i 的服务器上, C_{a_0} 的哈希值和由 C_{a_1}、C_{a_2} 构成了关键字索引作为交易存储在私有链上. 而由私有链块标识 ID_b、患者伪身份 ID_a 和关键字索引 (C_{a_1}, C_{a_2}) 构成的安全索引作为交易存储在联盟链上.

为了实现患者的匿名性, 医生为患者产生伪身份. 未经患者本人授权, 其他用户不能将伪身份与真实身份相关联. 不同医生为同一患者产生的伪身份也不同, 以实现不可链接性. 最后, 医生构建新交易, 并广播至医院私有链. 当收到该交易后, 私有链的验证者进行验证, 生成了如表 1 数据结构的新区块. 医院服务器提取私有链中每个新的块标识 ID_b、患者伪身份 ID_a 和关键字索引 (C_{a_1}, C_{a_2}) 构成安全索引 T_{X_a}. 其中 $T_{X_a}=(ID_b, ID_a, (C_{a_1}, C_{a_2}))$. 服务器将在私有链上收集到的 T_{X_a} 作为交易上传至联盟链, 联盟链上节点进行验证, 若验证通过, 生成如表 2 数据结构的新区块.

若去其他医院就诊, 当医生想要查看该患者相关的历史诊断记录时, 患者将搜索陷门 T_1 和 T_2 发送至联盟链, 联盟链上节点进行搜索. 若搜索成功, 联盟链上节点提取安全索引中的私有链块标识 ID_b. 且通过私有链块标识 ID_b, 联盟链上节点可以得到病历密文的哈希值, 由医院服务器进行密文哈希值对比得到病历密文并返回给联盟链上节点. 最后, 患者可用自己的私钥解密该密文.

当经过患者授权的数据用户要访问患者历史诊断记录数据时, 患者将搜索陷门发送到联盟链上进行关键字密文搜索. 若搜索成功, 联盟链上节点作为代理者进行代理重加密并将重加密密文发送给数据用户, 数据用户用自己的私钥进行解密获得患者的电子病历.

2.6 方案设计

本文方案由系统建立、数据产生与存储、数据搜索与访问 3 个步骤组成.

1) 系统建立:

本阶段系统运行参数生成算法生成公共参数 PP, 患者、医生和数据用户分别生成各自的公私钥对. 每次患者去医院就诊时, 医院选择随机数 $\beta\in Z_q^*$, 将 β 安全地发送给患者. 同时, 医院为该患者指定

一名医生, 计算 $\mu = H_1(\beta)$ 并发送到医院服务器.

a) 初始化:

系统输入安全参数 λ, 输出双线性对 $e: G_1 \times G_1 \to G_2$, 其中 G_1、G_2 是阶数为素数 q 的乘法循环群, 选择生成元 $g \in G_1$, 计算 $h = e(g, g)$. 定义 6 个哈希函数 $H_1: \{0, 1\}^* \to Z_p^*$、$H_2: \{0, 1\}^* \to G_1$、$H_3: \{0, 1\}^* \times \{0, 1\}^* \to G_1$、$H_4: G_2 \to \{0, 1\}^*$、$H_5: \{0, 1\}^* \times G_1 \to Z_p^*$ 和 $H_6: G_1 \to \{0, 1\}^*$. 设置公共参数 $PP = (g, h, e, q, G_1, G_2, H_1, H_2, H_3, H_4, H_5, H_6)$.

b) 密钥生成:

患者 a 随机选择 $x_a \in Z_q^*$ 作为私钥 sk_a, 并计算公钥 $pk_a = g^{x_a}$. 医生 d 随机选择 $x_d \in Z_q^*$ 作为其私钥 sk_d, 并计算公钥 $pk_d = g^{x_d}$. 数据用户 u 随机选择 $x_u \in Z_q^*$ 作为私钥 sk_u, 并计算其公钥 $pk_u = g^{x_u}$. 通过激励机制, 选择相应的联盟链上节点作为验证者运行搜索算法和作为代理者执行代理重加密算法. 同时联盟链上的节点选择 $x_s \in Z_q^*$ 作为私钥 sk_s, 计算公钥 $pk_s = g^{x_s}$.

c) 重加密密钥生成:

输入患者 a 和数据用户 u 的私钥 (sk_a, sk_u), 采用文献 [13] 的方法为代理者产生代理重加密密钥 $rk = sk_u/sk_a$.

2) 数据产生与存储:

当患者就诊时, 向医生出示 β, 医生对病患诊断后产生病历 $m \in \{0, 1\}^*$. 并提取关键字 $w \in \{0, 1\}^*$. 医生用患者的公钥 pk_a 加密 m 和 w. 具体步骤如下:

a) 加密:

输入病历 $m \in \{0, 1\}^*$ 和关键字 $w \in \{0, 1\}^*$, 医生随机选择 $r \in Z_q^*$, 计算 $B = pk_a^r$, $C = e(g^r, H_2(\beta)) \times m$, $t = e(g^r, H_3(\beta, w))$, $F = H_4(t)$.

计算向量 $\boldsymbol{X} = [X_1, X_2, \cdots, X_n]$, 其中 $X_1 = g^{rH_1(w)}$, $X_2 = g^{rH_1(w)^2}$, $\cdots$, $X_n = g^{rH_1(w)^n}$.

计算 $r_0 = H_5(w, B)$, $A = g^{rH_1(w) + r_0(sk_d + H_1(w))}$, $Y = h^{r_0(sk_d + H_1(w))}$.

记 $C_{a_0} = (B, C)$, $C_{a_1} = (B, F)$, $C_{a_2} = (A, Y, \boldsymbol{X})$. 其中, C_{a_0} 为电子病历 m 的密文, C_{a_1} 为关键字 w 的密文, C_{a_2} 为联盟链上的一致性证明提供了依据. C_{a_0} 存储在医院 i 的服务器上, 医生将 C_{a_0} 的哈希值和由 C_{a_1}、C_{a_2} 构成的关键字索引上传至私有链上.

b) 患者伪身份生成:

患者的真实身份为 RID_a, 医生随机选取 $k \in Z_q^*$, 计算患者伪身份 $ID_a = RID_a \oplus H_1(\beta)^k$ 并保密 k. 为了提供私有链上的一致性证明, 医生计算 $\eta = (\alpha = g^{k + sk_d/H_1(\beta)}, \beta' = H_6(g^k) \oplus \beta)$. 最后, 医生利用关键字索引、医生身份和医生签名来构建新交易并将交易广播至医院私有链. 收到新交易后, 私有链上的验证者对新交易进行验证: 从交易中提取 $\eta = (\alpha, \beta')$, 并在医院服务器中搜索 μ, 计算 $\beta^* = H_6(\alpha^{\mu} \cdot pk_d^{-1}) \oplus \beta'$, 检查 $\mu = H_1(\beta^*)$ 是否成立.

若等式成立, 则新交易有效, 验证者广播验证确认消息, 当收到 $[2/3np]$ 的验证确认消息之后, 私有链接受新交易, 并生成如表 1 数据结构的新区块. 否则, 拒绝新块加入私有链. $[np]$ 表示私有链中的节点数量.

正确性:

$$\begin{aligned} H_1(\beta^*) =& H_1(H_6(\alpha^{\mu} \cdot pk_D^{-1}) \oplus \beta') = \\ & H_1(H_6(g^{k + sk_d/H_1(\beta) \cdot H_1(\beta)} \cdot g^{-sk_d}) \oplus \beta') = \\ & H_1(H_6(g^{k + sk_d} \cdot g^{-sk_d}) \oplus \beta') = \\ & H_1(H_6(g^k) \oplus H_6(g^k) \oplus \beta) = H_1(\beta) = \mu \end{aligned}$$

c) 数据存储:

在每个私有链中, 服务器提取每个新块的块标识、患者伪身份和关键字索引, 令安全索引 $T_{X_a} = (ID_b, ID_a, (C_{a_1}, C_{a_2}))$, 服务器利用安全索引、服务器身份和服务器签名来构建新交易并将交易广播至联盟链.

收到新交易后, 联盟链上的验证者验证等式 $e\left(\prod_{i=0}^{i=n} X_i^{a_i}, X_2\right) = e(X_1, X_1)$ 和等式 $e(A, g) = e(X_1, g)Y$ 是否成立. 其中 a_i 为联盟链中的共识机制构造的多项式 $g(x) = a_n x^n + \cdots + a_1 x$ 的常数项. 若等式成立, 则新交易有效, 验证者广播验证确认消息, 当收到 $[2/3np]$ 的验证确认消息之后, 联盟链接受新交易, 并生成如表 2 数据结构的新区块. 否则, 拒绝新块加入联盟链. $[np]$ 表示联盟链中的节点数量.

正确性:

$$\begin{aligned} e\left(\prod_{i=0}^{n} X_i^{a_i}, X_2\right) &= e\left(\prod_{i=0}^{n} g^{ra_i H_1(w)^i}, g^{rH_1(w)^2}\right) = \\ & e\left(\prod_{i=0}^{n} g^{r(a_n H_1(w)^n + \cdots + a_1 H_1(w))}, g^{rH_1(w)^2}\right) = \\ & e\left(g^{r(\boldsymbol{ah})}, g^{rH_1(w)^2}\right) = e\left(g^r, g^{rH_1(w)^2}\right) = \\ & e\left(g^{rH_1(w)}, g^{rH_1(w)}\right) = e(X_1, X_1) \end{aligned}$$

$$\begin{aligned} e(A, g) =& e(g^{rH_1(w) + r_0(sk_d + H_1(w))}, g) = \\ & e(g^{rH_1(w)}, g) e(g^{r_0(sk_d + H_1(w))}, g) = \\ & e(X_1, g) e(g^{r_0(sk_d + H_1(w))}, g) = e(X_1, g)Y \end{aligned}$$

3) 数据搜索与访问:

当患者或数据用户想要访问病历数据时, 患者使用私钥为其产生搜索陷门并发送到联盟链. 具体

过程如下:

a) 陷门生成:

患者随机选择$r_w \in Z_q^*$,计算陷门 $T_1 = H_3(\beta, w)^{1/sk_a} pk_s^{r_w}$, $T_2 = g^{r_w}$.

b) 搜索:

联盟链上节点计算 $T_w = T_1/T_2^{sk_s}$ 并验证等式 $F = H_4(e(B, T_w))$ 是否成立. 若成立, 联盟链上节点提取安全索引 $T_{X_a} = (ID_b, ID_a, (C_{a_1}, C_{a_2}))$ 并获得私有链块标识 ID_b. 通过私有链块标识 ID_b, 联盟链上节点访问相应的私有链得到病历密文的哈希值, 由医院服务器进行密文哈希值对比后得到病历密文 C_{a_0}, 并将其返回给联盟链上节点.

正确性:

$$H_4(e(B, T_w)) = H_4\left(e\left(pk_a^r, \frac{T_1}{T_2^{sk_s}}\right)\right) = H_4\left(e\left(pk_a^r, \frac{H_3(\beta, w)^{\frac{1}{sk_a}} pk_s^{r_w}}{g^{r_w sk_s}}\right)\right) = H_4\left(e(pk_a^r, H_3(\beta, w)^{\frac{1}{sk_a}})\right) = H_4(e(g^r, H_3(\beta, w)) = H_4(t) = F$$

c) 解密:

情形 1. 当患者需要访问病历数据时, 联盟链上节点发送 C_{a_0} 给患者, 患者计算明文 $m = C/e(B, H_2(\beta))^{1/sk_a}$. 当医生需要访问病历数据时, 患者将明文 m 发送给医生.

正确性:

$$\frac{C}{e(B, H_2(\beta))^{\frac{1}{sk_a}}} = \frac{e(g^r, H_2(\beta))m}{e(g^{sk_a r}, H_2(\beta))^{\frac{1}{sk_a}}} = \frac{e(g^r, H_2(\beta))m}{e(g^r, H_2(\beta))} = m$$

情形 2. 当数据用户 u 共享数据时, 代理者产生代理重加密密钥 $rk = sk_u/sk_a$, 并用 rk 对密文 $C_{a_0} = (B, C)$ 进行重加密, 计算 $B' = B^{rk}$, 则重加密密文为 $C'_{a_0} = (B', C)$. 代理者将重加密密文 C'_{a_0} 发送给数据用户 u, 数据用户计算 $m = C/e(B', H_2(\beta))^{1/sk_u}$.

正确性:

$$\frac{C}{e(B', H_2(\beta))^{\frac{1}{sk_u}}} = \frac{C}{e(B^{rk}, H_2(\beta))^{\frac{1}{sk_u}}} = \frac{C}{e(g^{sk_a \frac{sk_u}{sk_a} r}, H_2(\beta))^{\frac{1}{sk_u}}} = \frac{e(g^r, H_2(\beta))m}{e(g^r, H_2(\beta))} = m$$

3 安全分析

本节分析本文提出方案如何有效地满足系统模型中提出的设计目标.

3.1 数据安全与访问控制

区块链的基本特性使得存储在区块链中的数据是不可更改的, 确保数据无法修改, 除非攻击者具有全网百分之五十一的计算能力. 电子病历密文是使用患者的公钥加密的, 因此只有用患者的私钥才能解密数据, 保证了数据的机密性. 本文构建私有链上新区块时附有医生的签名, 而在构建联盟链上新区块时附有医院的签名, 这保证了数据的完整性. 存储在区块链上的密文, 只允许经过身份验证的访问者获取. 若医生需要患者数据, 患者上传搜索陷门, 联盟链上节点进行搜索后返回密文给患者, 患者解密后给医生. 当数据用户访问数据时, 首先与患者和联盟链上节点交互得到代理重加密密钥, 而后联盟链上节点运行代理重加密算法得到重加密密文, 相当于患者对数据用户进行授权. 因此, 患者能够对自己的电子病历进行访问控制.

3.2 隐私保护

医生为患者生成的伪身份 $ID_a = RID_a \oplus H_1(\beta)^k$, 窃听者无法得到 β 和随机数 k, 无法推出患者的真实身份, 因此, 本文方案实现了匿名性和不可追踪性, 保护了患者的身份信息. 如表 2 所示, 私有链区块上附有患者伪身份; 如表 3 所示, 联盟链区块上的安全索引包含患者伪身份, 即使是同一个患者, 由于 k 的随机性, 则每次生成的患者伪身份不同. 因此, 窃听者无法判断两个或多个电子病历密文是否来自同一患者, 保证了数据的不可链接性. 表 3 中 ✓ 和 × 分别表示是否具有该功能.

3.3 安全搜索

在搜索过程中, 患者利用自己的私钥和联盟链上节点的公钥生成陷门, 联盟链上节点利用自己的私钥进行搜索. 因为陷门 T_1、T_2 涉及患者私钥 sk_a 和号码牌 β, 搜索算法中涉及了联盟链上节点私钥 sk_s, 即使窃听者得知陷门, 也无法推断出关键字和号码牌 β, 进而无法推断出患者的真实身份, 有助于抵抗关键词猜测攻击.

3.4 系统可用性

在联盟链上, 共识机制需要医院服务器提供证据验证关键字索引中的关键字属于关键字集. 若 C_{a_2}=$(A, Y, \boldsymbol{X})$ 可以通过等式 $e\left(\prod_{i=0}^{i=n} X_i^{a_i}, X_2\right) = e(X_1, X_1)$ 则等式 $\boldsymbol{ah} = 1$ 成立, 这意味着数据加密

表 3　功能特性比较

Table 3　Comparisons of functional properties

功能特性	文献 [5]	文献 [12]	文献 [25]	文献 [26]	文献 [27]	文献 [28]	本文方案
区块链	×	✓	✓	×	×	×	✓
访问控制	✓	✓	✓	✓	✓	✓	✓
隐私保护	✓	✓	✓	✓	✓	✓	✓
安全搜索	✓	✓	×	×	✓	✓	✓
第三方数据共享	×	×	×	×	✓	✓	✓

过程中使用的关键字属于关键字集 $W=\{w_1, w_2, \cdots, w_n\}$. 而且医生在构造证据 C_{a_2} 时使用的是关键字 w 的哈希值 $H_1(w)$, 由于哈希函数的单向性, 即使窃听者获得证据 $C_{a_2}=(A, Y, \boldsymbol{X})$, 但窃听者无法得到任何与关键字有关的信息. 在私有链上, 验证者通过验证患者是否由授权医生生成电子病历来确定新块的有效性. 虽然交易中包含患者的伪身份, 但患者的伪身份 $ID_a=RID_a\oplus H_1(\beta)^k$ 中 k 为随机数, 号码牌 β 保密, 故窃听者无法得到患者的真实身份.

4　性能分析

4.1　理论分析

1) 功能性对比

本文方案与文献 [5, 12, 25−28] 进行了功能性对比, 其中文献 [5, 12, 25−26] 皆应用于医疗电子病历, 而文献 [27−28] 的应用环境则是云服务器. 结果由表 3 所示. 对比发现文献 [5, 26−28]均为非区块链数据存储平台, 文献 [25] 与文献 [26]无法达成数据搜索功能, 文献 [5, 12, 25−26] 方案均不具备第三方数据用户安全共享患者数据的功能. 表中文献方案均满足方案的访问控制与隐私保护. 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.

2) 运算成本分析

在表 4 中, T_p 表示双线性配对运算的时间,T_e 表示指数运算的时间, T_m 表示乘法运算的时间, T_h 表示哈希运算的时间. 由表 2 可以看出, 常用密码操作配对时间的排序为 $T_p>T_e>T_m>T_h$, 且配对运算的时间 T_p 远大于其他密码操作的时间.

表 4　常用密码算法的计算成本 (ms)

Table 4　The computational cost of common cryptographic algorithms (ms)

操作	T_p	T_e	T_m	T_h
时间	4.064	1.655	0.013	0.006

由表 5 可以看出, 在关键字密文生成阶段, 各方案计算量由大到小依次为本文方案、文献 [28] 和文献 [27]; 在搜索阶段, 各方案计算量由大到小依次为文献 [27]、文献 [28] 和本文方案.

表 5　方案的计算代价

Table 5　Computational overhead of the proposed scheme

方案	数据加密	数据搜索
本文方案	$2T_p+8T_e+7T_h$	T_p+T_h
文献 [27]	$4T_e+2T_m+5T_h$	$2T_p+2T_e+2T_m+2T_h$
文献 [28]	$T_p+5T_e+T_h$	$T_p+T_e+T_m+2T_h$

本文方案应用在区块链上的医疗体系下. 假设 np 代表私有链或联盟链上的节点数量, 则在私有链一致性验证时, 本方案的计算开销是 $(T_e+T_m+2T_h)\times[2/3np]$, 在联盟链一致性验证时, 本文方案的计算开销是 $(4T_p+T_e+T_m)\times[2/3np]$.

4.2　数值模拟

数值模拟实验是在 Linux 虚拟机上通过利用 PBC (Paring-Based Cryptography) 库由 C 语言进行编写, 并在 2.50 GHz CPU、4 GB 内存笔记本电脑上运行. 在数值实验中, 由于本文、文献 [27]和文献 [28] 方案只支持单关键字的搜索, 设单关键字的基本字段长度为 1 024 位, 因此将变量设置为关键字的个数. 将变量分别设置为 10、20、30、40 和 50, 实验结果取 50 次运行结果的平均值, 实验结果如表 6 所示.

由表 6 的数值结果可以发现, 在系统建立和数据产生与存储阶段, 变量的增加对系统建立算法和私有链上对新块的验证算法所产生的时间成本基本没有影响, 加密算法和联盟链上对新块验证的算法因涉及了多个双线性对的运算, 故时间成本受到较大影响. 在数据搜索与访问阶段, 2 种情形下解密算法的时间开销基本没有影响, 搜索陷门产生算法和测试算法中双线性对的运算涉及比重较小, 大部分涉及点乘运算与幂运算, 因此时间成本增长较为缓慢.

为了更清晰地观察本文方案的性能优缺点, 对本文和文献 [27] 和文献 [28] 方案在数据加密与数据搜索算法的时间开销进行了分析, 如图 4 ~ 5 所示. 由图 4 可以看出, 尽管本文的加密算法时间开销要高于文献 [27] 和文献 [28] 方案, 但是本文更适用于区块链上的医疗体系. 由图 5可以看出, 随着关键字个数的增加, 3 个方案的时间开销呈现线性增

表 6 本方案算法各个阶段的时间成本 (毫秒)
Table 6 Time cost of each phase in the scheme (ms)

算法	系统建立	数据加密	私有链验证	联盟链验证	陷门生成	测试	解密 1	解密 2
$n = 10$	20	218	4	73	36	42	7	10
$n = 20$	21	412	3	142	72	83	8	11
$n = 30$	20	614	5	213	105	125	7	11
$n = 40$	20	825	4	285	145	167	7	11
$n = 50$	21	1 021	4	365	172	212	7	11

长, 且本文的搜索时间开销要较小于文献 [27] 和文献 [28] 方案. 故本文方案的搜索效率较高. 故本文方案在搜索计算代价上有较明显的优势, 提高了系统的性能.

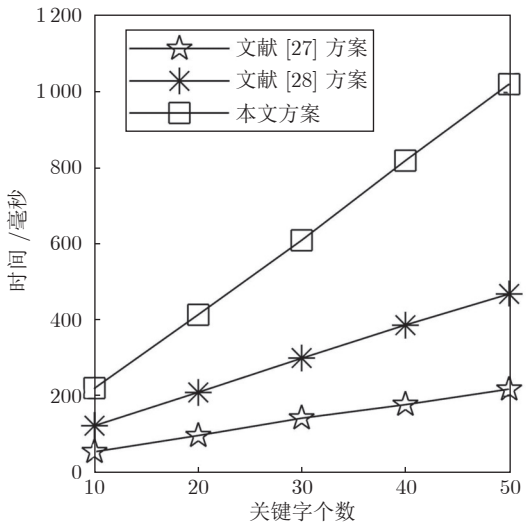

图 4 加密算法的时间成本
Fig. 4 Time cost of encryption algorithms

5 结束语

本文提出了一种基于区块链的电子病历数据共享方案, 用于第三方数据用户对患者数据的安全访问. 方案的构建是基于私有链与联盟链的, 每家医院拥有自己的私有链, 多家私有链一起构建联盟链. 服务器上存储患者电子病历密文, 私有链存储病历密文的哈希值和关键字索引, 联盟链存储由患者伪身份和关键字索引所构成的安全索引. 方案使用可搜索加密技术实现了联盟链上的安全搜索; 使用代理重加密完成对密文的转换, 使数据用户能对患者数据进行安全访问. 方案实现了数据安全、访问控制、隐私保护和安全搜索的安全目标. 最后, 通过数值实验分析了方案的综合性能水平. 在之后的工作

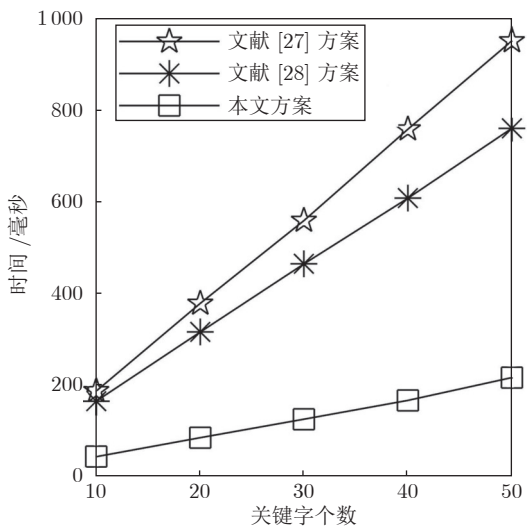

图 5 搜索算法的时间成本
Fig. 5 Time cost of search algorithms

中, 拟将方案的单关键字搜索加密改为链接关键字搜索加密, 并且进一步细化区块链上对新区块的验证过程.

References

1 Shahnaz A, Usman Q, Ayesha K. Using blockchain for electronic health records. *IEEE Access*, 2019, **7**: 147782−147795

2 Chen L, Lee W, Chang C, Choo K, Zhang N. Blockchain based searchable encryption for electronic health record sharing. *Future Generation Computer Systems*, 2019, **95**: 420−429

3 Hao W, Song Y. Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. *Journal of Medical Systems*, 2018, **18**(2): 152−161

4 Wang Y, Zhang A, Zhang P, Wang H. Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain. *IEEE Access*, 2019, **7**: 136704−136719

5 Yuan Yong, Ni Xiao-Chun, Zeng Shuai, Wang Fei-Yue. Blockchain consensus algorithms: The state of the art and future trends. *Acta Automatica Sinica*, 2018, **44**(11): 2011−2022
(袁勇, 倪晓春, 曾帅, 王飞跃. 区块链共识算法的发展现状与展望. 自动化学报, 2018, **44**(11): 2011−2022)

6 Han Xuan, Yuan Yong, Wang Fei-Yue. Security problems on blockchain: The state of the art and future trends. *Acta Automatica Sinica*, 2019, **45**(1): 206−225
(韩璇, 袁勇, 王飞跃. 区块链安全问题: 研究现状与展望. 自动化学报, 2019, **45**(1): 206−225)

7 Zeng Shuai, Yuan Yong, Ni Xiao-Chun, Wang Fei-Yue. Scaling blockchain towards bitcoin: Key technologies, constraints and related issues. *Acta Automatica Sinica*, 2019, **45**(6): 1015−1030
(曾帅, 袁勇, 倪晓春, 王飞跃. 面向比特币的区块链扩容: 关键技术, 制约因素与衍生问题. 自动化学报, 2019, **45**(6): 1015−1030)

8 Yue X, Wang H, Jin D, Li M, Jiang W. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *Journal of Medical Systems*, 2016, **40**(10): 218−226

9 Xia Q, Sifah E B, Smahi A, Amofa S, Zhang X. BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. *Information*, 2017, **8**(2): 44−60

10 Zhang Chao, Li Qiang, Chen Zi-Hao, Li Zu-Rui, Zhang Zhen. Medical chain: Alliance medical blockchain system. *Acta Automatica Sinica*, 2019, **45**(8): 1495−1510
(张超, 李强, 陈子豪, 黎祖睿, 张震. Medical Chain: 联盟式医疗区块链系统. 自动化学报, 2019, **45**(8): 1495−1510)

11 Chen Y, Ding S, Xu Z, Zheng H, Yang SS. Blockchain-based medical records secure storage and medical service framework. *Journal of Medical Systems*, 2019, **43**(1): 5−14

12 Zhang A, Lin Xiao-Dong. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *Journal of Medical Systems*, 2018, **42**(8): 140−158

13 Boneh D, Di Crescenzo G, Ostrovsky R, Persiano G. Public key encryption with keyword search. In: Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Germany: Heidelberg Springer, 2004. 506−522

14 Baek J, Safavi-Naini R, Susilo W. Public key encryption with keyword search revisited. In: Proceedings of the International conference on Computational Science and Its Applications. Berlin, Germany: Heidelberg Springer, 2008. 1249−1259

15 Hu C, Liu P. An enhanced searchable public key encryption scheme with a designated tester and its extensions. *Journal of Computer*, 2012, **7**(3): 716−723

16 Shao J, Cao Z, Liang X, Lin H. Proxy re-encryption with keyword search. *Information Science*, 2010, **180**(13): 2576−2587

17 Ryu E K, Takagi T. Efficient coSnjunctive keyword-searchable encryption. In: Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops. Niagara Falls, Canada: 2007, 1: 409−414

18 Boneh D, Waters B. Conjunctive, subset, and range queries on encrypted data. In: Proceedings of the Theory of Cryptography Conference. Berlin, Germany: Heidelberg Springer, 2007. 535−554

19 Blaze M, Bleumer G, Strauss M. Divertible protocols and atomic proxy cryptography. In: Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Germany: Heidelberg Springer, 1998. 127−144

20 Fang L, Susilo W, Ge C, Wang J. Chosen-ciphertext secure anonymous conditional proxy re-encryption with keyword search. *Theoretical Computer Science*, 2012, **462**: 39−58

21 Shao J, Cao Z. Multi-use unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption. *Information Sciences*, 2012, **206**: 83−95

22 Tang F, Li H, Chang J. Multi-hop unidirectional proxy re-encryption from multilinear maps. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 2015, **98**(2): 762−766

23 Liu Zhen-Hua, Zhou Pei-Lin, Duan Shu-Hong. Attribute-based proxy re-encryption scheme with keyword search. *Journal of Electronics and Information Technology*, 2018, **40**(3): 683−689
(刘振华, 周佩琳, 段淑红. 支持关键词搜索的属性代理重加密方案. 电子与信息学报, 2018, **40**(3): 683−689)

24 Ouyang Li-Wei, Wang Shuai, Yuan Yong, Ni Xiao-Chun, Wang Fei-Yue. Smart contracts: Architecture and research progresses. *Acta Automatica Sinica*, 2019, **45**(3): 445−457
(欧阳丽炜, 王帅, 袁勇, 倪晓春, 王飞跃. 智能合约:架构及进展. 自动化学报, 2019, **45**(3): 445−457)

25 Peterson K, Deeduvanu R, Kanjamala P, Boles K. A blockchain-based approach to health information exchange networks. In: Proceedings of the NIST Workshop Blockchain Healthcare. Berlin, Germany: Heidelberg Springer, 2016, 1: 1−10

26 Zhang J, Xue N, Huang X. A secure system for pervasive social network-based healthcare. *IEEE Access*, 2016, **4**: 9239−9250

27 Han Xiao, Zeng Qi, Cao Yong-Ming. An efficient proxy re-encryption scheme with keyword search. *Computer and Modernization*, 2019, **283**(03): 121−125
(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. 计算机与现代化, 2019, **283**(03): 121−125)

28 Guo Li-Feng, Li Ting. Improved proxy re-encryption with keyword search scheme. *Journal of Shanxi University (Natural Science Edition)*, 2016, **39**(3): 434−441
(郭丽峰, 李婷. 改进的带关键字搜索的代理重加密方案S. 山西大学学报(自然科学版), 2016, **39**(3): 434−441)

牛淑芬 西北师范大学计算机科学与工程学院副教授. 主要研究方向为密码学与信息安全.
E-mail: sfniu76@nwnu.edu.cn
(**NIU Shu-Fen** Associate professor at the School of Computer Science and Engineering, Northwest Normal University. Her research interest covers cryptography and information security.)

陈俐霞 西北师范大学计算机科学与工程学院硕士研究生, 主要研究方向为密码学. 本文通信作者.
E-mail: chenlx78@163.com
(**CHEN Li-Xia** Master student at the School of Computer Science and Engineering, Northwest Normal University. Her main research interest is cryptography. Corresponding author of this paper.)

李文婷 西北师范大学计算机科学与工程学院硕士研究生. 主要研究方向为密码学.
E-mail: wenting_li201@163.com
(**LI Wen-Ting** Master student at the School of Computer Science and Engineering, Northwest Normal University. Her main research interest is cryptography.)

王彩芬 西北师范大学计算机科学与工程学院教授. 主要研究方向为密码学和信息安全.
E-mail: wangcf@nwnu.edu.cn
(**WANG Cai-Fen** Professor at the School of Computer Science and Engineering, Northwest Normal University. Her research interest covers cryptography and information security.)

杜小妮 西北师范大学数学与统计学院教授. 主要研究方向为信息安全, 密码学和编码.
E-mail: ymldxn@126.com
(**DU Xiao-Ni** Professor at the School of Mathematics and Statistics, Northwest Normal University. Her research interest covers information security, cryptography and coding.)