基于联盟链的可搜索加密电子病历数据共享方案

牛淑芬[1]，刘文科[1]，陈俐霞[1]，王彩芬[1]，杜小妮[2]
（1. 西北师范大学计算机科学与工程学院，甘肃 兰州 730070；
2. 西北师范大学数学与统计学院，甘肃 兰州 730070）

摘 要：针对云存储电子病历（EMR）中病历数据难以在不同医院间共享的问题，提出了一种区块链上基于可搜索加密的 EMR 数据共享方案。该方案使用服务器存储 EMR 密文，私有链存储密文哈希值，联盟链存储关键字索引，以实现 EMR 的安全存储与共享。利用可搜索加密技术实现在联盟链上对关键字的安全搜索，利用代理重加密技术实现其他数据用户对患者 EMR 的数据共享。安全性分析表明，所提方案满足密文安全和关键字安全。此外，通过功能分析、计算效率分析和数值模拟对所提方案进行了性能分析。性能分析表明，该方案具有较高的计算效率。

关键词：区块链；电子病历；可搜索加密；代理重加密；数据共享
中图分类号：TP309.7
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2020116

Electronic medical record data sharing scheme based on searchable encryption via consortium blockchain

NIU Shufen[1], LIU Wenke[1], CHEN Lixia[1], WANG Caifen[1], DU Xiaoni[2]
1. College of Computer Science and Engineering, Northwest Normal University, Lanzhou 730070, China
2. College of Mathematics and Statistics, Northwest Normal University, Lanzhou 730070, China

Abstract: Considering that it was difficult to share medical record data among different medical institutions in cloud storage, an electronic medical record data sharing scheme based on searchable encryption on blockchain was proposed. In order to realize the secure storage and sharing of electronic medical records in the scheme, the patient's electronic medical record ciphertext was stored in the hospital server, the ciphertext hash value was stored in the private blockchain, and the keyword index was stored in the consortium blockchain. Searchable encryption was used to implement secure search of keywords in the consortium blockchain, and proxy re-encryption technology was used to realize the sharing of electronic medical records of patients by other data users. Security analysis shows that the proposed scheme can achieve ciphertext security and keyword security. Moreover, the performance of the scheme was analyzed by function analysis, computational efficiency analysis and numerical simulation. The performance analysis shows that the scheme can achieve high computational efficiency.

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

1 引言

电子病历（EMR, electronic medical record）使用数字化方式创建、存储和使用个人健康状况和保健信息。传统的 EMR 是将数据存储在医院本地服务器，在占用大量设备的同时，也不便于数据共享。云计算可以实现对海量数据的分析处理，提供可靠的数据处理与存储中心，越来越多的医院选择将其 EMR 存储到云服务器中，而不是维护一个专门的数据中心[1]。但是，由于数据泄露或未经授权的访问等安全问题，云服务器不能完全被用户信任。EMR 涉及大量的患者隐私信息，因此防止 EMR

收稿日期：2020−01−08；**修回日期**：2020−05−15
基金项目：国家自然科学基金资助项目（No.61562077, No.61662069, No.61662071, No.61772022）
Foundation Item: The National Natural Science Foundation of China (No.61562077, No.61662069, No.61662071, No.61772022)

内容被未经授权的用户和云服务器获取是非常重要的。

考虑到云服务器的不可靠性和用户数据的隐私性，需要对数据进行加密后再外包至云服务器。利用可搜索加密技术实现对加密数据的搜索，使 EMR 的使用更加便利。但是，医院只允许其授权的用户对云服务器中的数据进行访问，这导致云服务器中数据的使用具有局限性。

为了解决上述问题，文献[2-5]将区块链技术应用于医疗领域，将患者的 EMR 数据上传至区块链，实现对 EMR 数据的访问和共享。区块链是一个经过验证的、不可变的分布式账本，用于存储 EMR 记录。此外，该技术跟踪记录所有的交易，保证了数据交换过程中的透明性。因此，用区块链来存储 EMR，可以使患者对自己的病历数据的管理更加便利。区块链去中心化和开放的特性使患者能够掌握自己的医疗健康信息，这不仅保护了患者的隐私，也保证了患者对其医疗数据的访问控制。例如，患者可以在自己的 EMR 中记录医生的医疗和诊断信息，从而便于之后的诊断。

2　相关工作

随着云计算的飞速发展，云计算中的安全问题日益凸显，因此人们对访问控制[6-7]和隐私保护[8-9]等安全问题进行了一系列的研究。云存储作为云计算中的一部分，既能保证数据安全，又能实现搜索功能。为了解决对密文的直接搜索问题，Song 等[10]首先提出了基于流密码和对称加密的可搜索加密方案，但该方案只允许持有私钥的用户才能对数据进行加密和搜索，不满足人们的实际需求。为解决这一问题，Boneh 等[11]提出了公钥可搜索加密（PEKS, public key encryption with keyword search）方案，即公钥加密与可搜索加密的结合。Wu 等[12]提出一种新的不需要安全通道的可搜索加密（SCF-PEKS, secure channel free searchable encryption）方案，并将其应用至 EMR 中以实现对 EMR 的共享。可搜索加密实现了从加密数据中检索密文，而代理重加密技术将加密数据共享给更多用户。Shao 等[13]首次提出支持关键字搜索的代理重加密（PRES, proxy re-encryption with keyword search）方案，将 PEKS 和代理重加密技术结合，实现了第三方授权用户对密文的获取与解密。Liu 等[14]结合属性加密和可搜索加密技术，并将其应用至 EMR 中，实现了对 EMR 数据的存储、模糊搜索和共享。由于医院对云服务器的限制，这些应用于 EMR 的方案大多没有涉及不同医院之间的数据共享。

区块链的发展为上述问题带来了解决方案，其去中心化的分布式存储结构适用于医疗数据的共享。Xia 等[15]提出了一种基于许可链的医疗数据共享框架，只允许被邀请和经过验证的用户进行访问。Yue 等[16]提出了一个被称为医疗数据网关的应用程序，将私有链作为云存储的角色进行数据存储，并确保患者拥有和控制他们的医疗数据。Zhang 等[17]通过构造联盟链与私有链，提出了一种基于区块链的安全隐私保护个人健康信息共享方案。

本文以 EMR 的安全存储、隐私保护和安全共享为目标，将可搜索加密和代理重加密技术结合区块链应用于 EMR，用以实现 EMR 在不同医院间的共享和患者对 EMR 数据的访问控制。该方案特点如下：1) 方案中 EMR 由医生产生，医生将 EMR 加密后上传至医院服务器，医院服务器将密文哈希值放至私有链，确保 EMR 的安全存储；2) 医生使用可搜索加密技术加密关键字上传至联盟链，患者使用其私钥生成搜索陷门发送至联盟链，联盟链负责搜索；3) 联盟链节点使用代理重加密技术对 EMR 密文进行重加密，生成 EMR 重加密密文，经过患者授权的数据用户可使用其私钥解密重加密密文得到 EMR。为保护患者隐私，整个共享过程使用患者的伪身份。

3　预备知识

3.1　双线性映射

定义 1　令 G_1 和 G_2 为 2 个阶为素数 q 的加法循环群，定义一个双线性映射 $e: G_1 \times G_1 \to G_2$，其满足以下性质。

1) 双线性。对于任意 $a,b \in Z_q^*$ 和 $x,y \in G_1$，有 $e(ax,by)=e(x,y)^{ab}$。

2) 非退化性。存在 $x,y \in G_1$，使 $e(x,y) \neq 1$。

3) 可计算性。对于任意的 $x,y \in G_1$，存在有效算法来计算 $e(x,y)$。

3.2　困难性假设

定义 2　计算性 Diffie-Hellman（CDH, computational Diffie-Hellman）问题。对于任意 $a,b \in Z_q^*$，给定 $P, aP, bP \in G_1$，CDH 问题就是计算 abP。

定义 3 判定性 Diffie-Hellman（DDH, decision Diffie-Hellman）问题。对于任意 $a,b \in Z_q^*$，给定 $P, aP, bP, T \in G_1$，DDH 问题就是判断 $T = abP$ 是否成立。

3.3 区块链技术

区块链是通过区块链接在一起的有序记录的列表[18]，其本质上是一个分散的数据库，是分布式数据存储、点对点传输、协商共识机制、加密算法等计算机技术的一种新的应用模式。区块链也是一个分布式账本，并使用密码学方法使其不能被篡改。

根据区块链网络中心化程度的不同，可将其分为 3 种模式：公有链（public blockchain）、联盟链（consortium blockchain）和私有链（private blockchain）。公有链是完全去中心化、无许可的区块链，任何节点都可进入和获取信息，例如比特币和以太坊。联盟链是部分去中心化的区块链，通常由多个机构共同管理，只有经过机构授权的用户才可以访问。私有链是完全中心化的区块链，由一个中心机构控制访问权限。本文方案中，各个医院在联盟链上进行 EMR 数据共享。每家医院拥有自己的服务器和私有链，服务器上存储 EMR 密文，私有链上存储 EMR 密文的哈希值，多家医院组成联盟并创建一个联盟链用以存储患者 EMR 的安全索引。

本文中区块链合法的区块由区块头、区块体、签名和时间戳组成。区块头由 4 部分组成：区块 ID、区块大小、前一个区块的哈希值和 Merkle 树，其中，区块 ID 表示每个区块唯一的身份；区块大小显示区块占用的存储空间；前一个区块的哈希值用于链接前一个区块，防止区块链被修改；Merkle 树用于快速归纳和校验区块数据的存在性和完整性。区块体中是交易单（TX, transaction），本文中，私有链区块结构与联盟链区块结构唯一的不同之处是交易单的结构，这部分内容将在第 4 节中说明。签名用于验证区块的完整性。时间戳表示区块的生成时间。

4 本文方案

本节介绍基于联盟链的 EMR 存储与共享模型及其方案，给出区块链上的交易单结构，并提出安全目标。

4.1 基于联盟链的 EMR 存储与共享模型

本文模型中 n 家医院协商构建一个联盟链，每家医院都拥有服务器和私有链。医院服务器中存储患者的 EMR 密文，私有链中存储 EMR 密文的哈希值，联盟链中存储关键字密文。图 1 为 EMR 共享系统模型，系统模型中有 6 个实体：患者、医生、其他数据用户、医院服务器、私有链和联盟链。图 1 中 β 为就诊号，c_{a0} 为电子病历密文，hash(c_{a0}) 为 c_{a0} 的哈希值。

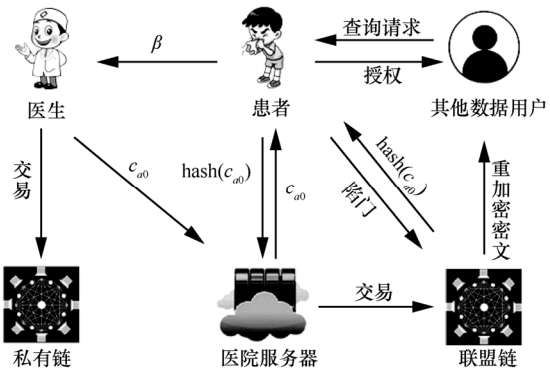

图 1 EMR 共享系统模型

患者。当患者去医院就诊时，首先需要注册，医院服务器为其生成就诊号。患者就诊时将就诊号交给医生，作为其对医生的授权。医生对患者诊断后为患者生成 EMR，将 EMR 加密后上传至服务器进行存储。患者在不同医院就诊时，其 EMR 密文的哈希值就存储在医院的私有链中。同时，每家医院将其存储在私有链中的关键字密文发送至联盟链。患者可在联盟链中搜索关键字来获取其 EMR，若医生需要，则将 EMR 交给医生。

医生。在得到患者授权后，医生对患者进行诊断，为其生成 EMR 和伪身份，构建证据，为私有链提供一致性证明，并将 EMR 加密后存储至服务器。同时，医生构建包含密文的哈希值、医生身份、患者伪身份、关键字索引和证据的交易单，并将交易单上传至私有链。另外，医生在对患者诊断时，也需了解患者以往的就诊记录，以便得出更加精确的诊断结果。

其他数据用户。当其他数据用户想要获取某患者的 EMR 时，需获得该患者的授权。在与其他数据用户和患者交互后，联盟链上节点生成代理重加密密钥，联盟链上节点使用重加密密钥对 EMR 密文重加密，生成重加密密文，其他数据用户使用其私钥即可解密。

医院服务器。每家医院都拥有一台服务器和维护服务器的多台客户端，医生使用客户端将患者的 EMR 存储在服务器中。医院服务器构建私有链的新

区块，用以存储包括病人信息相关的 EMR 数据交易单。医院服务器也负责为联盟链构建新区块，新区块构建完成后，其他医院服务器负责验证新区块的有效性。

私有链。每家医院都拥有私有链，医生使用患者 EMR 构建交易单并上传至私有链。在搜索阶段，患者发送搜索陷门至联盟链，联盟链搜索后通过私有链身份定位至私有链，获取 EMR 密文的哈希值。

联盟链。多家医院协商构建联盟链，医院服务器使用关键字密文、患者伪身份和私有链身份构建安全索引，使用安全索引构建交易单后将交易单上传至联盟链。在搜索阶段，收到患者发送的陷门后，联盟链上节点负责执行搜索，并返回 EMR 密文的哈希值给患者。患者可登录医院服务器进行哈希值比对，若一致，服务器返回 EMR 密文给患者；否则，服务器返回查询失败给患者。同时，联盟链上节点还负责为其他数据用户生成 EMR 重加密密文。

4.2　区块链上 EMR 交易单结构

私有链上交易单由 4 部分组成：病历生成者（医生）ID、病历拥有者（患者）ID、病历关键字索引和病历密文哈希值，如表 1 所示。为了保护患者的隐私，病历是以密文的形式存储的。其中，病历拥有者 ID 是患者的伪身份，由患者真实身份计算而来。

表 1　　**私有链上交易单**

病历生成者 ID	病历拥有者 ID	病历关键字索引	病历密文哈希值
ID_d	ID_a	(c_{a1},c_{a2})	$hash(c_{a0})$

联盟链上交易单由 2 部分组成：区块生成者（医院服务器）ID 和安全索引，如表 2 所示。医院服务器收集医生发送的关键字密文，利用构建的安全索引创建新的区块。联盟链区块的区块体中不存储原始 EMR，而是存储包含关键字密文的安全索引。安全索引 Tx_a 由 3 部分组成：私有链区块 ID_b、患者伪 ID_a 和关键字密文 c_{a1}。

表 2　　**联盟链上交易单**

区块生成者 ID	安全索引
ID_h	Tx_a=(ID_b,ID_a,c_{a1})

4.3　安全目标

假设本文方案中医院服务器为半可信的，其可能会尝试解密密文。同时，一些恶意攻击者可能会在传输期间拦截、修改或伪造 EMR 数据。外部攻击者可能入侵医院服务器或客户端，窃取存储的文件。考虑上述威胁模型，本文方案的安全目标如下。

数据的机密性和完整性。无论患者的 EMR 是存储在医院服务器还是通过公共渠道进行传输，其他实体都无法读取或修改患者的 EMR。通常数据的机密性和完整性是通过加密和签名来保证的。本文方案通过使用私有链存储 EMR 和联盟链存储关键字来保证数据的安全性。

访问控制。为防止未授权用户对 EMR 数据进行访问，对 EMR 的访问受控制，使数据访问活动始终在患者和医院的参与和监控之下进行。并通过对密码原语进行标识、身份认证和授权来实现访问控制。

安全搜索。当医生想要获取患者的历史 EMR 数据时，患者生成搜索陷门对 EMR 进行搜索。在搜索过程中，只有患者才能生成搜索陷门从而进行搜索。同时，搜索过程中使用患者的伪身份，窃听者也无法推断出患者的真实身份。

隐私保护。由于 EMR 中包含患者的一些隐私敏感信息，因此共享 EMR 的同时也要保护患者的身份隐私。此外，原始的 EMR 不能透露给非法实体。

4.4　基于联盟链的 EMR 存储与共享方案

基于联盟链的 EMR 存储与共享方案可分为 3 个阶段：系统建立、数据加密与存储、数据搜索与解密。

阶段 1　系统建立

本阶段分为初始化和密钥生成 2 个步骤。

1) 初始化。给定安全参数 λ，输出系统参数 $SP=(G,q,P,e,h)$。其中，G 是阶为素数 q 的加法循环群，P 为 G 的生成元，e 为双线性映射，令 $h=e(P,P)$，5 个哈希函数分别为 $H_0:G\to\{0,1\}^*$，$H_1:\{0,1\}^*\to Z_q^*, H_2:G\to M, H_3:M\times G\to Z_q^*$，$H_4:G\times Z_q^*\times G\to Z_q^*$。

2) 密钥生成。输入系统参数 SP，患者 a 随机选择 $(k_{a1},k_{a2},k_{a3})\in Z_q^*$ 作为其私钥 sk_a，计算 $K_{a1}=k_{a1}P$，$K_{a2}=k_{a2}P$，$K_{a3}=k_{a3}P$，则公钥为 $pk_a=(K_{a1},K_{a2},K_{a3})$；医生 d 随机选择 $k_d\in Z_q^*$ 作为其私钥 sk_d，计算 $K_d=k_dP$，则公钥为 $pk_d=(K_d)$；其他数据用户 u 随机选择 $k_u\in Z_q^*$ 作为其私钥 sk_u，

计算 $K_u = k_u P$，则公钥为 $\mathrm{pk}_u = (K_u)$。

阶段 2 数据加密与存储

本阶段分为患者注册、数据加密、私有链交易单生成和联盟链交易单生成 4 个步骤。

1) 患者注册。患者 a 到医院 h 就诊时，向医院服务器申请注册。医院服务器生成 $\beta \in \{0,1\}^*$ 秘密发送给患者，并计算 $\mu = H_1(\beta)$ 存储至系统中。患者就诊时向医生 d 出示 β，医生为患者生成伪随机身份 $\mathrm{ID}_a = \mathrm{RID}_a \oplus H_1(\beta)$，其中 $\mathrm{RID}_a \in Z_q^*$ 为患者真实身份。

2) 数据加密。在对患者完成诊断后，医生为其产生病历 $m \in \{0,1\}^*$ 和关键字 $w \in \{0,1\}^*$。医生加密病历 m 和关键字 w 如下。

① 随机选择 $r_1 \in Z_q^*$，计算 $B = r_1 K_{a2}$，$r_0 = H_3(m, B)$，$A = r_0(K_{a1} + H_1(w)P) + r_1 H_1(w)P$，$E = r_0 K_{a3}$，$F = H_4(h^{r_0}, A, B)$。

②计算 $J = h^{r_0(k_{a1} + H_1(w))}$ 和向量 $\boldsymbol{X} = [X_1, X_2, \cdots, X_n]$，其中 $X_1 = r_1 H_1(w)P$，$X_2 = r_1 (H_1(w))^2 P, \cdots, X_n = r_1 (H_1(w))^n P$。

③计算 $c_m = H_2(e(P,P)^{r_0 + r_1}) \oplus m$，记 $c_{a0} = (c_m, B)$，$c_{a1} = (A, B, E, F)$，$c_{a2} = (J, \boldsymbol{X})$，$c_e = (A, J, \boldsymbol{X})$。其中，$c_{a0}$ 为 EMR m 的密文，医生上传 c_{a0} 至医院服务器，服务器计算 c_{a0} 的哈希值 $\mathrm{hash}(c_{a0})$ 并存储在医院私有链上；c_{a1} 为关键字 w 的密文；c_e 为联盟链提供一致性证明的证据。

3) 私有链交易单生成

①医生构建交易单 TX 如表 1 所示。交易单 TX 中包含 ID_d、ID_a、(c_{a1}, c_{a2}) 和 $\mathrm{hash}(c_{a0})$。

②医生随机选择 $r \in Z_q^*$，计算 $\alpha = \dfrac{r}{k_d + H_1(\beta)}$，$\beta' = H_0(rP) \oplus \beta$。记证据为 $\eta = (\alpha, \beta')$，其中 η 为私有链提供的一致性证明。

医生广播交易单 TX 至医院私有链。一旦医院私有链接收到新交易，私有链的验证者进行验证，过程如下。

①从私有链区块中提取 ID_d 和 $\eta = (\alpha, \beta')$，在医院系统中搜索与 ID_d 匹配的 μ。

②计算 $\beta^* = H_0\big(\alpha(K_d + \mu P)\big) \oplus \beta'$，验证等式 $H_1(\beta^*) = \mu$ 是否成立。若等式成立，则验证者接收交易单，广播验证确认信息。在接收到超过 $\left\lceil \dfrac{2}{3} n_p \right\rceil$ 的验证信息后，新交易被接收，并添加到私有链上。否则，私有链拒绝该交易。其中，n_p 表示节点数量。

4) 联盟链交易单生成。在每个私有链上，医院服务器生成安全索引 $\mathrm{Tx}_a = (\mathrm{ID}_b, \mathrm{ID}_a, c_{a1})$，用来构建如表 2 所示的交易单 TX。服务器广播交易单 TX 和 c_{a2} 至联盟链上。当收到新交易，联盟链的验证者验证等式 $e(A,P) = e(X_1,P)J$ 和等式 $e(\boldsymbol{aX}, X_2) = e(X_1, X_1)$ 是否成立。若等式成立，则验证者接收交易，广播验证确认信息。在接收到超过 $\left\lceil \dfrac{2}{3} n_p \right\rceil$ 的验证信息之后，新交易被接收，并添加到联盟链上。否则，联盟链拒绝该交易。其中，向量 $\boldsymbol{a} = (a_n, \cdots, a_1)$ 为文献[17]中联盟链共识机制构造的多项式 $g(x) = a_n x^n + \cdots + a_1 x$ 中的系数。

阶段 3 数据搜索与解密

本阶段分为陷门生成、搜索和解密 3 个步骤。患者就诊时，为了进行更精确的诊断，医生需查看患者的历史诊断记录。患者生成搜索陷门 T，发送 T 和 ID_a 至联盟链。联盟链上节点运行搜索算法获取 EMR 密文的哈希值并将其发送给患者，患者可通过登录医院服务器获取 EMR 密文。患者得到密文后，使用其私钥进行解密，得到 EMR 明文后交给医生查看。除了患者可获取其 EMR 外，经患者授权的其他数据用户也可获取患者 EMR，在解密步骤中分别叙述。

1) 陷门生成。患者生成搜索陷门 $T = (T_1, T_2)$ 过程如下，计算 $T_1 = \dfrac{P}{k_{a1} + H_1(w) + k_{a3}\mathrm{ID}_a}$，$T_2 = \dfrac{T_1}{k_{a2}}$。

2) 搜索。一旦收到患者的搜索陷门 T 和患者伪随机身份 ID_a，联盟链上节点提取安全索引 $\mathrm{Tx}_a = (\mathrm{ID}_b, \mathrm{ID}_a, c_{a1})$，匹配患者的伪随机身份 ID_a。联盟链上节点进行验证，过程如下。

① 计算 $U_1 = e(A + \mathrm{ID}_a E, T_1)$，$U_2 = e(B, T_2)^{H_1(w)}$。

② 计算 $V = \dfrac{U_1}{U_2}$，验证等式 $H_4(V, A, B) = F$。若等式成立，联盟链上节点通过私有链身份 ID_b 定位至私有链获取 $\mathrm{hash}(c_{a0})$；否则，联盟链上节点返回搜索失败。

3) 解密。解密过程分为患者获取 EMR 和其他数据用户获取 EMR 共 2 种情形。

情形 1 当患者需获取 EMR 时，联盟链上节点

发送 hash(c_{a0}) 和 V 给患者，患者登录医院服务器获取密文 $c_{a0}=(c_m,B)$，得到 c_{a0} 后计算 $c_m \oplus H_2\left(Ve(P,B)^{\frac{1}{k_{a2}}}\right)=m$，$m$ 即为该患者的 EMR。

情形 2　当其他数据用户想获取某位患者的 EMR 时，首先与患者和联盟链进行交互，生成代理重加密密钥 $rk_{a\to u}=\dfrac{k_u}{k_{a2}}$。患者将 c_{a0} 发送给联盟链，联盟链节点使用 $rk_{a\to u}$ 对密文 c_{a0} 进行重加密，计算 $B'=B^{rk_{a\to u}}=B^{\frac{k_u}{k_{a2}}}=r_1K_u$，生成重加密密文 $c'_{a0}=(c_m,B')$。联盟链上节点将重加密密文 $c_{a0}{}'$ 和 V 发送给其他数据用户，其他数据用户计算 $c_m \oplus \ H_2\left(Ve(P,B')^{\frac{1}{k_u}}\right)=m$。

4.5　正确性分析

本文的正确性分析如下。

1) 私有链交易单生成 H

$$H_1(\beta^*)=H_1\left(H_0\left(\alpha(K_d+\mu P)\right)\oplus\beta'\right)=$$
$$H_1\left(H_0\left(\frac{r}{k_d+H_1(\beta)}\left(k_dP+H_1(\beta)P\right)\right)\oplus H_0(rP)\oplus\beta\right)=$$
$$H_1\left(H_0(rP)\oplus H_0(rP)\oplus\beta\right)=H_1(\beta)=\mu$$

2) 联盟链交易单生成

$$e(A,P)=e\left(r_0\left(K_{a1}+H_1(w)P\right)+r_1H_1(w)P,P\right)=$$
$$e\left(r_1H_1(w)P,P\right)e\left(r_0(K_{a1}+H_1(w)P),P\right)=$$
$$e(X_1,P)e(P,P)^{r_0\left(k_{a1}+H_1(w)\right)}=e(X_1,P)J$$

$$e(\boldsymbol{aX},X_2)=$$
$$e\Big(a_1r_1H_1(w)P+a_2r_1\left(H_1(w)\right)^2P+\cdots+$$
$$a_nr_1\left(H_1(w)\right)^nP,r_1\left(H_1(w)\right)^2P\Big)=e\left(r_1P,r_1\left(H_1(w)\right)^2P\right)=$$
$$e\left(r_1H_1(w)P,r_1H_1(w)P\right)=e(X_1,X_1)$$

3) 搜索

$$V=\frac{U_1}{U_2}=\frac{e(A+\mathrm{ID}_aE,T_1)}{e(B,T_2)^{H_1(w)}}=$$
$$\frac{e\left(r_0\left(K_{a1}+H_1(w)P\right)+r_1H_1(w)P+\mathrm{ID}_ar_0K_{a3},T_1\right)}{e\left(r_1K_{a2},\dfrac{T_1}{k_{a2}}\right)^{H_1(w)}}=$$
$$\frac{e\left(r_0P\left(k_{a1}+H_1(w)+\mathrm{ID}_ak_{a3}\right)+r_1H_1(w)P,T_1\right)}{e\left(r_1P,T_1\right)^{H_1(w)}}=$$
$$\frac{e\left(r_0P\left(k_{a1}+H_1(w)+\mathrm{ID}_ak_{a3}\right),T_1\right)e\left(r_1H_1(w)P,T_1\right)}{e\left(r_1PH_1(w),T_1\right)}=$$
$$e\left(r_0P\left(k_{a1}+H_1(w)+\mathrm{ID}_ak_{a3}\right),\frac{P}{k_{a1}+H_1(w)+\mathrm{ID}_ak_{a3}}\right)=$$
$$e\left(r_0P,P\right)=e\left(P,P\right)^{r_0}=h^{r_0}$$

4) 解密

情形 1

$$c_m\oplus H_2\left(Ve(P,B)^{\frac{1}{k_{a2}}}\right)=H_2\left(e(P,P)^{r_0+r_1}\right)\oplus m\oplus$$
$$H_2\left(e(P,P)^{r_0}e(P,r_1K_{a2})^{\frac{1}{k_{a2}}}\right)=$$
$$H_2\left(e(P,P)^{r_0+r_1}\right)\oplus m\oplus H_2\left(e(P,P)^{r_0}e(P,P)^{r_1}\right)=m$$

情形 2

$$c_m\oplus H_2\left(Ve(P,B')^{\frac{1}{k_u}}\right)=$$
$$H_2\left(e(P,P)^{r_0+r_1}\right)\oplus m\oplus H_2\left(e(P,P)^{r_0}e(P,r_1K_u)^{\frac{1}{k_u}}\right)=$$
$$H_2\left(e(P,P)^{r_0+r_1}\right)\oplus m\oplus H_2\left(e(P,P)^{r_0}e(P,P)^{r_1}\right)=m$$

5　安全性分析

本文方案在实现安全目标的同时，又能满足密文安全和关键字安全。

5.1　安全目标

数据的机密性和完整性。EMR 数据在上传到医院服务器存储之前是经过加密的。医生使用患者的公钥对 EMR 进行加密，解密时 $m=c_m\oplus H_2\left(Ve(P,B)^{\frac{1}{k_{a2}}}\right)$，由于 k_{a2} 为患者的私钥，故只有患者可进行解密，这实现了 EMR 数据的机密性。另外，区块链中的数据是不可变的，若数据添加或交易已经完成，它就不能被编辑或删除，构建的新区块上存在区块生成者的签名，实现了 EMR 数据的完整性。

访问控制。EMR 密文的哈希值存储在私有链，只允许经过身份验证的人员访问；EMR 密文存储在医院服务器，用户必须在医院注册后并经过身份验证才能访问数据。患者上传搜索陷门 $T=(T_1,T_2)$，

联盟链上节点验证通过后，发送密文的哈希值 $\text{hash}(c_{a0})$ 给患者，患者登录医院服务器即可获取 EMR 密文。只有拥有私钥，才能生成搜索陷门 $T_1=\dfrac{P}{k_{a1}+H_1(w)+k_{a3}\text{ID}_a}$ 和解密 EMR 密文 c_{a0}，因此患者可以控制 EMR 的访问。

安全搜索。阶段 2 数据的加密及存储过程中，EMR 和关键字都是以密文形式进行存储，其他实体无法获取关键字。阶段 3 数据搜索与解密过程中，患者生成搜索陷门 $T=(T_1,T_2)$ 发送给联盟链，其中 T_1 包含患者的私钥，只有患者能够生成，故其他用户无法知道搜索结果。

隐私保护。首先，EMR 由医生上传至私有链，上传的交易单中包含患者的伪身份 ID_a，伪身份 $\text{ID}_a=\text{RID}_a\oplus H_1(\beta)$ 由医生生成，患者的真实身份 RID_a 和 β 无法被获取。其次，数据的搜索过程中也只包含患者的伪身份，因此，此方案中公共信息不会泄露患者的真实身份，实现了对患者身份的隐私保护。

5.2 安全性证明

5.2.1 密文安全

定理 1 若敌手 A_1 在一个概率多项式时间内能以不可忽略的优势 ε 赢得游戏，则挑战者 B 能够以不可忽略的优势 $\dfrac{\varepsilon}{2}$ 解决 DDH 困难问题。

证明 假设给挑战者 B 一个 DDH 实例 (aP,bP,cP)，挑战者 B 的目的是确定 $cP=abP$ 是否成立。游戏过程如下。

1) 系统建立。挑战者 B 选择 P 作为群 G 的生成元，q 为群 G 的阶，则双线性对为 $e:G\times G\to G_T$。挑战者 B 选择随机数 $r_1\in Z_q^*$。

2) 哈希询问阶段。挑战者 B 建立如下哈希询问。

$O_{H_1}(W)$。敌手 A_1 输入关键字 W，挑战者 B 从列表 L_{H_1} 中恢复数组 $(W,r^{(1)},R^{(1)})$，若 $R^{(1)}$ 不为空值，挑战者 B 提取 $R^{(1)}$ 发送给敌手 A_1。否则，挑战者 B 选择随机数 $r^{(1)}\in Z_p^*$，计算 $R=r^{(1)}$ 记入列表 L_{H_1} 中数组 $(W,r^{(1)},R^{(1)})$。

$O_{H_2}(Q)$。敌手 A_1 输入 Q，挑战者 B 从列表 L_{H_2} 中恢复数组 $(Q,r^{(2)},R^{(2)},\beta)$，若 $R^{(2)}$ 不为空值，挑战者 B 提取 $R^{(2)}$ 发送给敌手 A_1。否则，挑战者 B 选择随机数 $r^{(2)}\in Z_q^*$ 并设置 $R^{(2)}=r^{(2)}$ 记入数组 $\left(Q,r^{(2)},R^{(2)},\beta\right)$。

$O_{H_3}\left(m,B\right)$。敌手 A_1 输入 m,B，挑战者 B 从列表 L_{H_3} 中恢复数组 $\left(m,B,r^{(3)},R^{(3)},\beta\right)$，若 $R^{(3)}$ 不为空值，挑战者 B 提取 $R^{(3)}$ 发送给敌手 A_1。否则，挑战者 B 从列表 L^{list} 中恢复数组 $(\text{ID},K_{a1},K_{a2},K_{a3},k_{a1},k_{a2},k_{a3},\beta)$ 得到 β 值。若 $\beta=1$，挑战者 B 选择随机数 $r^{(3)}\in Z_q^*$ 并设置 $R^{(3)}=r^{(3)}$ 记入数组 $(m,B,r^{(3)},R^{(3)},\beta)$。否则，挑战者 B 设置 $R^{(3)}=b-r_1$。

$O_{H_4}\left(V,A,B\right)$。敌手 A_1 输入 V,A,B，挑战者 B 从列表 L_{H_4} 中恢复数组 $\left(V,A,B,r^{(4)},R^{(4)}\right)$，若 $R^{(4)}$ 不为空值，挑战者 B 提取 $R^{(4)}$ 发送给敌手 A_1。否则，挑战者 B 选择随机数 $r^{(4)}\in Z_p^*$ 并设置 $R^{(4)}=r^{(4)}$ 记入数组 $\left(V,A,B,r^{(4)},R^{(4)}\right)$。

3) 询问阶段。敌手 A_1 发起了多项式次数内的私钥询问和陷门询问。

$O_{\text{pk}}\left(\text{SP},\text{ID}\right)$。敌手 A_1 输入系统参数 SP 和用户伪身份 ID 给挑战者 B。挑战者 B 从列表 L^{list} 中恢复数组 $(\text{ID},K_{a1},K_{a2},K_{a3},k_{a1},k_{a2},k_{a3},\beta)$，若 K_{a1},K_{a2},K_{a3} 不为空值，挑战者 B 提取 K_{a1},K_{a2},K_{a3} 发送给敌手 A_1。否则，挑战者 B 选择随机数 $k_{a1},k_{a2},k_{a3},k_d\in Z_q^*$，计算医生公钥为 $K_d=k_dP$ 并抛掷一个硬币 $\beta\in\{0,1\}$。若正面朝上，则 $\beta=1$，挑战者 B 设置用户公钥 $K_{a1}=k_{a1}P$，$K_{a2}=k_{a2}P$，$K_{a3}=k_{a3}P$ 并记入数组 $(\text{ID},K_{a1},K_{a2},K_{a3},k_{a1},k_{a2},k_{a3},\beta)$；否则 $\beta=0$，挑战者设置用户公钥 $K_{a1}=k_{a1}P$，$K_{a2}=k_{a2}P$，$K_{a3}=k_{a3}P$ 并记入数组 $(\text{ID},K_{a1},K_{a2},K_{a3},k_{a1},k_{a2},k_{a3},\beta)$。

$O_{\text{sk}}(\text{SP},\text{ID})$。敌手 A_1 输入系统参数 SP 和用户伪身份 ID 给挑战者 B。挑战者 B 从列表 L^{list} 中恢复数组 $(\text{ID},K_{a1},K_{a2},K_{a3},k_{a1},k_{a2},k_{a3},\beta)$，若 $\beta=1$，挑战者 B 回复私钥 k_{a1},k_{a2},k_{a3} 给敌手；否则 $\beta=0$，挑战者输出失败。

$O_{\text{te}}(\text{Tx}_a,T,\text{ID})$。挑战者 B 输入患者的搜索陷门 T、用户伪身份 ID 和安全索引并从列表 L^{list} 中恢复数组 $(\text{ID},K_{a1},K_{a2},K_{a3},k_{a1},k_{a2},k_{a3},\beta)$ 得到 β 值。若 $\beta=1$，挑战者运行搜索算法并将结果返回给敌手 A_1；否则 $\beta=0$，挑战者输出失败。

$O_{\text{dec}}(c_{a0},V)$。挑战者 B 输入密文并从列表 L^{list} 中恢复数组 $(\text{ID},K_{a1},K_{a2},K_{a3},k_{a1},k_{a2},k_{a3},\beta)$。若

$\beta=1$，挑战者 B 计算明文 $m=c_{a0}\oplus H_2(V^{k_{a2}})$ 返回给敌手；否则 $\beta=0$，挑战者输出失败。

4) 挑战。当询问阶段 1 完毕，敌手 A_1 选择 2 个明文 (m_0,m_1) 和挑战者伪身份 ID^* 一起发送给挑战者 B。挑战者 B 从列表 L^{list} 中恢复数组 $(\mathrm{ID}^*,K_{a1}{}^*,K_{a2}{}^*,K_{a3}{}^*,k_{a1}{}^*,k_{a2}{}^*,k_{a3}{}^*,\beta^*)$，若 $\beta^*=1$，挑战者 B 输出失败（该事件用 E 表示）；否则，挑战者 B 随机选取 $\delta\in\{0,1\}$，设置密文如下。

$$c_{a0}{}^*=H_2\left(e(P,aP)^b\right)\oplus m_\delta=H_2\left(e(P,K_{a2}{}^*)^{r^{(3)}+r_1}\right)\oplus m_\delta$$

$$B^*=r_1aP=r_1K_{a2}{}^*$$

$$A^*=r^{(3)}\left(K_{a1}{}^*+H_1(w)P\right)+r_1^*H_1(w)P=(b-r_1)K_{a1}{}^*+br^{(1)}P$$

$$E^*=r^{(3)}K_{a3}{}^*=(b-r_1)K_{a3}{}^*$$

$$F^*=H_4\left(h^{r^{(3)}},A^*,B^*\right)=H_4\left(h^{b-r_1},A^*,B^*\right)$$

$$c_{a1}{}^*=(A^*,B^*,E^*,F^*)$$

5) 询问阶段 2。敌手 A_1 进行询问，除挑战密文及其衍生不能询问外，其他同询问阶段 1 一致。

6) 猜测。最后，敌手 A_1 返回猜测 δ'，如果 $\delta'=\delta$，则挑战成功，输出 1；否则，输出 0。

分析。若事件 E 没有发生，敌手能攻破方案，则挑战者能解决 DDH 困难问题。当 $\beta=0$，则密文 $c_{a0}{}^*=H_2\left(e(P,abP)\right)\oplus m_\delta$ 是一个 DDH 实例，敌手的优势为 $\varepsilon=\Pr[\delta'=\delta]-\frac{1}{2}$，挑战者获胜的概率 $\Pr[\delta'=\delta\mid\beta=1]=\Pr[\delta'=\delta]=\varepsilon+\frac{1}{2}$。否则，事件 E 发生，挑战者获胜的概率 $\Pr[\delta'=\delta\mid\beta=0]=\Pr[\delta'\neq\delta]=\frac{1}{2}$，那么挑战者能解决 DDH 困难问题的优势为

$$\mathrm{Adv}=\Pr[\delta'=\delta]-\frac{1}{2}=\frac{1}{2}\left(\Pr[\delta'=\delta\mid\beta=1]+\Pr[\delta'=\delta\mid\beta=0]\right)-\frac{1}{2}=\frac{\varepsilon}{2}$$

5.2.2 关键字安全

定理 2　若敌手 A_2 在一个概率多项式时间内能以不可忽略的优势 ε 赢得游戏，则证明挑战者 B 能够以不可忽略的优势 $\frac{\varepsilon}{e(q_T+1)}$ 解决 CDH 困难问题。其中，敌手最多进行 $q_T>0$ 次陷门询问。

证明　假设给挑战者 B 一个 CDH 实例 (aP,bP)，挑战者 B 的目的是计算 abP 是否成立。游戏过程如下。

1) 系统建立。挑战者 B 选择 P 作为群 G 的生成元，q 为群 G 的阶，则双线性对为 $e:G\times G\to G_T$，随机数为 $u\in Z_p^*$。最后，敌手 A_2 输出挑战伪身份 ID，挑战者 B 设置数组 $(\mathrm{ID},W,u,R^{(3)},\beta)$ 放入列表 L^{list} 中，此时 W、$R^{(1)}$、$R^{(3)}$、β 为空值。

2) 哈希阶段。挑战者 B 建立如下哈希询问。

$O_{H_1}(W)$。敌手 A_2 输入关键字 W，挑战者 B 从列表 L_{H_1} 中恢复数组 $(W,r^{(1)},R^{(1)})$，若 W,R 不为空值，挑战者 B 提取 R 发送给敌手 A_2。否则，挑战者 B 选择随机数 $r^{(1)}\in Z_p^*$ 并抛掷一个硬币 $\beta\in\{0,1\}$，其中正面朝上的概率为 $\frac{1}{q_T+1}$。若正面朝上，则 $\beta=1$，挑战者设置 $R^{(1)}=a$ 记入数组 $(W,r^{(1)},R^{(1)})$；否则 $\beta=0$，挑战者设置 $R^{(1)}=r^{(1)}$ 记入数组 $(W,r^{(1)},R^{(1)})$。

$O_{H_3}(m,B)$。敌手 A_1 输入 m,B，挑战者 B 从列表 L^{list} 中恢复数组 $(\mathrm{ID},W,u,R^{(3)},\beta)$，若 $R^{(3)}$ 不为空值，挑战者 B 提取 $R^{(3)}$ 发送给敌手 A_1。否则，挑战者查看 β 值。若 $\beta=1$，挑战者设置 $R^{(3)}=b-u$ 记入数组 $(\mathrm{ID},W,u,R^{(3)},\beta)$；否则，挑战者 B 选择随机数 $r^{(3)}\in Z_p^*$，并设置 $R^{(3)}=r^{(3)}$ 记入数组 $(\mathrm{ID},W,u,R^{(3)},\beta)$。

$O_{H_4}(V,A,B)$。敌手 A_1 输入 V,A,B，挑战者 B 从列表 L_{H_4} 中恢复数组 $(V,A,B,r^{(4)},R^{(4)})$，若 $R^{(4)}$ 不为空值，挑战者 B 提取 $R^{(4)}$ 发送给敌手 A_1；否则，挑战者 B 选择随机数 $r^{(4)}\in Z_p^*$，并设置 $R^{(4)}=r^{(4)}$ 记入数组 $(V,A,B,r^{(4)},R^{(4)})$。

3) 询问阶段。敌手 A_2 发起了多项式次数的私钥询问和陷门询问。

$O_{\text{pk}}(\mathrm{SP},\mathrm{ID})$。敌手 A_1 输入系统参数 SP 和用户伪身份 ID 给挑战者 B。挑战者 B 选择随机数 $k_{a1},k_{a2},k_{a3},k_d\in Z_q^*$，计算医生公钥为 $K_d=k_dP$，用户公钥为 $K_{a1}=k_{a1}P$，$K_{a2}=k_{a2}P$，$K_{a3}=k_{a3}P$。

$O_{\text{sk}}(\mathrm{SP},\mathrm{ID})$。敌手 A_1 输入系统参数 SP 和用户伪身份 ID 给挑战者 B。挑战者 B 从列表 L^{list} 中恢复数组 $(\mathrm{ID},W,u,R^{(3)},\beta)$ 得到 β 值，若 $\beta=1$，挑战者 B 回复私钥 k_{a1},k_{a2},k_{a3} 给敌手；否则，挑战者输出失败。

$O_{\text{Trapdoor}}(W)$。敌手 A_2 输入关键字 W，挑战者 B 从列表 L^{list} 中恢复数组 $(\mathrm{ID},W,u,R^{(3)},\beta)$。若 $\beta=1$，

挑战者 B 输出失败；若 $\beta=0$，挑战者设置陷门 $T_1=\dfrac{P}{k_{a1}+b-R^{(3)}+k_{a3}\mathrm{ID}}=\dfrac{P}{k_{a1}+H_1(w)+k_{a3}\mathrm{ID}}$，$T_2=\dfrac{T_1}{k_{a2}}$，并发送给敌手 A_2。

4) 挑战。当询问阶段 1 完毕，敌手 A_2 选择 2 个关键字 (w_0,w_1) 和挑战身份 ID* 发送给挑战者 B。挑战者 B 询问 2 次 $O_{H_2}(W)$ 获得 $R_0=H_2(w_0)$, $R_1=H_2(w_1)$，而且在列表 L^{list} 中存在 2 个对应数组 $(\mathrm{ID}^*,W^*,u^*,R^{(3)*},\beta^*)$。若 $\beta_0=0$ 和 $\beta_1=0$ 同时发生，挑战者 B 输出失败；否则，挑战者 B 随机选取 $\delta\in\{0,1\}$ 且 $\beta_\delta=1$，挑战者 B 回应关键字索引 $c_{a1}{}^*=(A^*,B^*,E^*,F^*)$，其中

$$A^*=r^{(3)}\left(K_{a1}+H_1(w^*)P\right)+r_1H_1(w^*)P=(b-u^*)\cdot(K_{a1}{}^*+aP)+u^*aP=abP+(b-u^*)K_{a1}{}^*$$

$$B^*=u^*P=r_1K_{a2}{}^*$$

$$E^*=r^{(3)}K_{a3}{}^*=(b-u^*)K_{a3}{}^*$$

$$F^*=H_4(h^{r^{(3)}},A^*,B^*)=H_4(h^{b-u^*},A^*,B^*)$$

5) 询问阶段 2。敌手 A_2 进行询问，除挑战密文及其衍生不能询问外，其他与询问阶段 1 一致。

6) 猜测。最后，敌手返回猜测 δ'，如果 $\delta'=\delta$，则挑战者返回 $A^*-(b-u^*)K_{a1}{}^*$，挑战成功，输出 1；否则，输出 0。

分析。若 $\delta'=\delta$，则挑战者返回的 $A^*-(b-u^*)K_{a1}{}^*=abP$ 是 CDH 困难问题的实例，挑战成功。而该前提是挑战者在游戏过程中不终止，这意味着在陷门询问过程和挑战过程没有输出失败。在陷门询问过程，由于 $\beta=1$ 发生的概率为 $\dfrac{1}{q_T+1}$，而敌手最多进行 $q_T>0$ 次陷门询问，事件 E 发生的概率为 $\Pr[E]\geqslant\left(1-\dfrac{1}{1+q_T}\right)^{q_T}\geqslant\dfrac{1}{e}$。在挑战过程中，当 $\beta=0$ 输出失败，则挑战顺利的概率 $\Pr[\mathrm{challenge}]=\dfrac{1}{q_T+1}$。由于敌手的优势为 ε，那么挑战者能解决 CDH 困难问题的优势为

$$\mathrm{Adv}=\Pr[E]\Pr[\mathrm{challenge}]\varepsilon\geqslant\frac{\varepsilon}{e(q_T+1)}$$

6 性能分析

本节首先将本文方案与相关 EMR 方案的功能进行比较。然后，从理论角度分析本文方案的计算效率，并与已有的可搜索加密方案进行比较。最后，通过数值模拟实验对方案性能进行评估。

6.1 功能性分析

基于云存储的文献[12,19]方案、基于区块链的文献[20-21]方案与本文方案的功能性分析如表 3 所示。由表 3 可知，所有的方案都能实现访问控制和隐私保护的特性，这是 EMR 共享方案的关键安全目标。但文献[20]方案不能实现安全搜索，文献[12,20-21]方案不能实现身份认证。

表 3 功能性分析

方案	区块链	访问控制	隐私保护	安全搜索	身份认证
文献[12]	×	√	√	√	×
文献[19]	×	√	√	√	√
文献[20]	√	√	√	×	×
文献[21]	√	√	√	√	×
本文方案	√	√	√	√	√

6.2 计算效率理论分析

本节从理论角度分析本文方案与文献[12,22]方案在计算效率上的优劣。表 4 显示方案中基本运算的符号和执行时间。由表 4 可以看出，基本运算的执行时间的排序为 $T_h>T_p>T_e>T_H$。由于计算开销中指数运算、配对运算和哈希运算时间较长，故只考虑这 3 个方面的运算时间。下面，本文将利用表 4 中的数据得出各阶段的运行时间。

表 4 方案中的运算符号和执行时间

符号	描述	执行时间/ms
T_e	指数运算时间	4.888
T_p	双线性配对运算时间	5.021
T_h	一般哈希函数运算时间	12.573
T_H	哈希到点运算时间	0.008

表 5 显示加密、搜索和解密 3 个阶段的运算时间。由表 5 可以看出，在加密阶段，各方案计算量由大到小依次为文献[12]方案、文献[22]方案、本文方案；在搜索阶段，各方案计算量由大到小依次为文献[22]方案、文献[12]方案、本文方案；在解密阶段，各方案计算量由大到小依次为文献[22]方案、文献[12]方案、本文方案。

6.3 数值分析

本节对本文方案中算法进行数值模拟实验，并通过改变关键字的数量分析本文方案的计算效率，

表 5　　各阶段计算量对比

方案	加密阶段/ms	搜索阶段/ms	解密阶段/ms
文献[12]	$3T_e+T_p+T_h$=32.258	$2T_e+T_h$=22.349	T_e+2T_p=14.93
文献[22]	$T_e+2T_h+4T_H$=30.066	$3T_p+2T_h$=40.209	$T_e+4T_p+T_h+2T_H$=24.996
本文方案	$3T_e+T_p+4T_H$=19.717	$T_e+2T_p+2T_H$=14.946	$T_e+T_p+T_H$=9.917

表 6　　本文方案中算法的执行时间

关键字数量	系统构建/ms	数据加密/ms	私有链验证/ms	联盟链验证/ms	陷门生成/ms	关键字搜索/ms	数据解密/ms
n=10	37	309	15	226	92	148	1
n=50	37	1 455	15	1 155	457	744	1
n=100	37	2 977	15	2 319	903	1 456	1

关键字数量 n 分别取 10、50、100。数值模拟实验是在 Linux 操作系统下利用双线性包（pairing-based cryptography library）实现的，使用 C 语言对算法进行编程，在 PC 机（惠普电脑，3.1 GHz CPU，4 GB RAM）的虚拟机环境中运行。实验结果取算法运行 50 次的平均值，如表 6 所示。

系统构建算法模拟系统建立和患者注册阶段，数据加密算法模拟对 EMR 和关键字的加密过程，私有链验证算法模拟验证者对私有链上新区块验证的过程，联盟链验证算法模拟验证者对联盟链上新区块验证的过程，陷门生成算法模拟患者生成搜索陷门的过程，关键字搜索算法模拟联盟链匹配关键字的过程，数据解密算法模拟患者对 EMR 密文进行解密的过程。

由表 6 可知，由于数据加密、联盟链验证、陷门生成和关键字搜索算法中包含关键字信息，故这些算法的执行时间随着关键字的数量增加而增加；当关键字数量发生变化时，系统构建、私有链验证和数据解密算法的执行时间则不受其影响。

7　结束语

本文基于可搜索加密和代理重加密技术，提出了一种具有隐私保护和安全存储的 EMR 数据共享方案，解决了区块链上 EMR 共享过程中的数据安全和个人隐私等关键问题。在本文提出的区块链 EMR 共享模型中，医院服务器存储 EMR 密文、医院私有链存储 EMR 密文哈希值、联盟链存储关键字密文，实现了对 EMR 数据的安全存储与共享。其次，本文设计 EMR 区块链的数据结构和一致性证明，保证了所提方案的高效运行。另外，使用关键字搜索保证了数据的安全性和可搜索性。最后，安全性分析和性能分析表明，本文方案在达到设计的安全目标的同时还具有良好的性能。

参考文献：

[1] LI M, YU S, REN K, et al. Securing personal health records in cloud computing: patient-centric and fine-grained data access control in multi-owner settings[C]//International Conference on Security and Privacy in Communication Systems. Berlin: Springer, 2010: 89-106.

[2] ESPOSITO C, DE SANTIS A, TORTORA G, et al. Blockchain: a panacea for healthcare cloud-based data security and privacy?[J]. IEEE Cloud Computing, 2018, 5(1): 31-37.

[3] NOVO O. Blockchain meets IoT: an architecture for scalable access management in IoT[J]. IEEE Internet of Things Journal, 2018, 5(2): 1184-1195.

[4] WANG J, LI M, HE Y, et al. A blockchain based privacy-preserving incentive mechanism in crowdsensing applications[J]. IEEE Access, 2018, 6: 17545-17556.

[5] LIU P T S. Medical record system using blockchain, big data and tokenization[C]//International Conference on Information and Communications Security. Berlin: Springer, 2016: 254-261.

[6] YANG K, HAN Q, LI H, et al. An efficient and fine-grained big data access control scheme with privacy-preserving policy[J]. IEEE Internet of Things Journal, 2016, 4(2): 563-571.

[7] CAI Z, YAN H, LI P, et al. Towards secure and flexible EHR sharing in mobile health cloud under static assumptions[J]. Cluster Computing, 2017, 20(3): 2415-2422.

[8] LI T, LI J, LIU Z, et al. Differentially private Naive Bayes learning over multiple data sources[J]. Information Sciences, 2018, 444: 89-104.

[9] SHEN J, GUI Z, JI S, et al. Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks[J]. Journal of Network and Computer Applications, 2018, 106: 117-123.

[10] SONG D X, WAGNER D, PERRIG A. Practical techniques for searches on encrypted data[C]//Proceeding 2000 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2000: 44-55.

[11] BONEH D, DI CRESCENZO G, OSTROVSKY R, et al. Public key encryption with keyword search[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Sprin-

ger, 2004: 506-522.
[12] WU Y, LU X, SU J, et al. An efficient searchable encryption against keyword guessing attacks for sharable electronic medical records in cloud-based system[J]. Journal of Medical Systems, 2016, 40(12): 1-9.
[13] SHAO J, CAO Z, LIANG X, et al. Proxy re-encryption with keyword search[J]. Information Sciences, 2010, 180(13): 2576-2587.
[14] LIU Z, WENG J, LI J, et al. Cloud-based electronic health record system supporting fuzzy keyword search[J]. Soft Computing, 2016, 20(8): 3243-3255.
[15] XIA Q, SIFAH E B, SAMAHI A, et al. BBDS: blockchain-based data sharing for electronic medical records in cloud environments[J]. Information, 2017, 8(2): 44-60.
[16] YUE X, WANG H, JIN D, et al. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control[J]. Journal of Medical Systems, 2016, 40(10): 218-226.
[17] ZHANG A, LIN X. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain[J]. Journal of Medical Systems, 2018, 42(8): 140-154.
[18] MUKHOPADHYAY U, SKJELLUM A, HAMBOLU O, et al. A brief survey of cryptocurrency systems[C]// 2016 14th Annual Conference on Privacy, Security and Trust. Piscataway: IEEE Press, 2016: 745-752.
[19] WANG X, ZHANG A, XIE X, et al. Secure-aware and privacy-preserving electronic health record searching in cloud environment[J]. International Journal of Communication Systems, 2019, 32(8): e3925.
[20] AMOFA S, SIFAH E B, KWAME O B, et al. A blockchain-based architecture framework for secure sharing of personal health data[C]//2018 IEEE 20th International Conference on e-Health Networking, Applications and Services. Piscataway: IEEE Press, 2018: 1-6.
[21] LIU J, LI X, YE L, et al. BPDS: a blockchain based privaords[C]//2018IEEE Global Communications Conference. Piscataway: IEEE Press, 2018: 1-6.
[22] WANG Y, ZHANG A, ZHANG P, et al. Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain[J]. IEEE Access, 2019, 7: 136704-136719.

[作者简介]

牛淑芬（1976– ），女，甘肃兰州人，博士，西北师范大学副教授，主要研究方向为密码学、云计算、大数据网络的隐私保护。

刘文科（1996– ），男，安徽阜阳人，西北师范大学硕士生，主要研究方向为密码学。

陈俐霞（1996– ），女，江西九江人，西北师范大学硕士生，主要研究方向为密码学。

王彩芬（1963– ），女，河北安国人，博士，西北师范大学教授，主要研究方向为密码学、信息安全等。

杜小妮（1972– ），女，甘肃庆阳人，博士，西北师范大学教授，主要研究方向为对称密码、编码理论等。