面向医疗数据分享的轻量级且安全的搜索方案

谢晴晴[1]，宋亮晴[1]，冯霞[2]
（1.江苏大学计算机科学与通信工程学院，江苏 镇江 212013；2.海南大学网络空间安全学院（密码学院），海南 海口 570228）

摘 要：为了兼顾医疗数据的可用性与安全性，设计了一套轻量级且安全的搜索方案。所提搜索算法仅涉及两次配对和一次乘法运算，能够在利用智能合约执行搜索时兼顾低消耗和安全性要求。另外，该方案采用密钥策略属性基加密对搜索操作进行细粒度控制，并利用轻量级加密算法和外包解密机制降低用户终端的计算开销。最后，安全性分析和实验评估证明了所提方案的安全性和可行性。

关键词：医疗数据分享；轻量级；安全搜索；智能合约
中图分类号：TP309
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2024203

Lightweight and secure search scheme for medical data sharing

XIE Qingqing[1], SONG Liangqing[1], FENG Xia[2]
1. School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China
2. School of Cyberspace Security (School of Cryptology), Hainan University, Haikou 570228, China

Abstract: To balance the availability and security of medical data, a lightweight and secure search scheme was designed. The proposed search algorithm involved only two pairings and one multiplication operation, allowing for low consumption and security requirements when executing searches using smart contract. Additionally, the scheme employed key policy attribute-based encryption for fine-grained control over search operations, and utilized lightweight encryption algorithm and outsourced decryption mechanism to reduce computational overhead on user terminals. Finally, security analysis and experimental evaluations demonstrated the security and feasibility of the proposed scheme.

Keywords: medical data sharing, lightweight, secure search, smart contract

0 引言

电子病历（EMR, electronic medical record）能够显著提升医疗服务的效率。首先，EMR 可以让医生随时随地通过互联网了解患者的完整病史。其次，EMR 解决了信息孤岛问题，促进了不同医院之间的协作。另外，EMR 作为医学研究机构（MRI, medical research institution）的重要数据来源，为疾病预防、药物研发和临床实践提供了科学依据。

然而，EMR 通常包含个人身份、家庭地址、健康状况、诊断和治疗等敏感信息，因此 EMR 的分享很容易造成隐私泄露，并引发身份盗窃和医疗纠纷等问题[1]。为了保护患者的隐私，数据加密是一项关键措施，但是加密数据的分享将降低 EMR 的可用性。因此，平衡 EMR 的安全性和可用性仍然是一个亟待解决的问题。

为了平衡安全性和数据可用性，可搜索加密（SE, searchable encryption）[2]作为一项允许用户在

收稿日期：2024–06–05；修回日期：2024–11–08
通信作者：谢晴晴，xieqq@ujs.edu.cn
基金项目：国家自然科学基金资助项目（No.62002139, No.62272203）；江苏省自然科学基金资助项目（No.BK20200886）
Foundation Items：The National Natural Science Foundation of China (No.62002139, No.62272203), The Natural Science Foundation of Jiangsu Province (No.BK20200886)

加密数据上进行搜索的重要机制被提出并广泛应用。目前，一些学者在可搜索加密方面做了大量工作，如单关键字搜索[3]、多关键字搜索[4]、模糊关键字搜索[5]等。为了进一步实现细粒度访问控制，又有学者将SE技术与密文策略属性基加密（CP-ABE, ciphertext-policy attribute-based encryption）相结合[6-9]。然而，CP-ABE侧重于限制数据使用者的访问权限。在本文的应用场景中，主要聚焦于MRI对数据的特定属性需求，只有符合MRI特定属性需求的数据才需要被解密，从而避免解密不必要数据而造成的计算资源浪费。因此，基于CP-ABE的搜索方案并不适用于本文的应用场景。

本文将密钥策略属性基加密（KP-ABE, key-policy attribute-based encryption）方案与SE算法相结合。然而，两者的直接结合既不高效也不安全。目前，在大多数现有的SE算法中，检索操作交给云服务器执行，这依赖于云服务器必须诚实地遵循预定义的搜索协议，但是在恶意云服务器的场景下，搜索结果的正确性和完整性就无法保证，即存在搜索安全性问题。而使用区块链智能合约代替云服务器执行搜索可以解决这一安全性问题[10-12]。但是大多数现有的可搜索加密方案涉及的计算量较大，往往超过区块链智能合约可以承受的范围，即智能合约无法高效地实现当前的SE算法。尤其针对医疗大数据的背景，如何解决可搜索加密方案计算量大，超出区块链智能合约承受范围这一问题，实现既高效又安全的搜索仍是一个巨大的挑战。

为了解决这一挑战，本文提出了一个轻量级且安全的搜索方案。首先，设计了一套轻量级的可搜索加密协议，其中搜索算法仅包括两次配对和一次乘法运算，其计算的轻量级为区块链智能合约的使用提供了便利。而且利用区块链智能合约进行数据检索，避免了云服务器执行搜索所存在的欺诈行为，从而保证了搜索结果的正确性与完整性。其次，本文将其与KP-ABE方案相结合，使MRI能够按需获取符合搜索和特定属性需求的数据，即支持按需服务，两者的结合实现了轻量级可控搜索，确保了MRI只能解密符合其特定属性需求的搜索结果，兼顾了数据的有效利用和患者的隐私保护。最后，本文利用轻量级加密算法和外包解密机制来降低医院和MRI的计算开销。

本文的主要贡献如下。

1) 设计了轻量级搜索算法，仅需两次配对和一次乘法运算，降低了智能合约的计算开销，能更好地适应资源受限的场景，同时实现了在不需要不可信第三方参与情况下的安全搜索。

2) 提出了一个轻量级且安全的医疗数据分享方案，通过改进可搜索加密并将其与KP-ABE结合，实现高效且可控的数据搜索，以达到数据安全性和可用性的平衡。

3) 采用轻量级加密算法和外包解密机制，降低医院和MRI的计算开销，以满足用户端的轻量级计算需求。

4) 通过形式化的证明，表明本文方案可以抵抗选择明文攻击（CPA, chosen plaintext attacks）和关键字猜测攻击（KGA, keyword guess attacks）。同时实验评估证明了本文方案在搜索操作、医院加密和MRI解密方面的轻量级特点。

1　相关工作

1.1　基于区块链的医疗数据分享

区块链技术因其分布式、防篡改等特点，在医疗领域的应用和研究中备受关注。Lai等[13]将区块链技术与环签名算法相结合，实现了医疗数据的隐私保护和可追溯分享。Huang等[14]提出了一种基于区块链的医疗数据分享系统，采用代理重加密技术保护医疗数据隐私，并使用零知识证明对数据进行验证，在确保供需一致性的同时保护了医疗数据隐私。Kaur等[15]提出了一个多方医院数据分享方案，利用区块链技术和基于身份代理重加密算法确保医疗数据的隐私性和完整性。Liu等[16]利用区块链技术和属性基加密技术设计了一套医疗数据安全分享方案。该方案在确保数据隐私性的同时具备数据防篡改功能，并且能够避免单点故障问题的发生。Tang等[11]讨论了如何利用区块链和可搜索加密技术创建安全高效的医疗数据分享平台，他们提出的方案着重于允许用户在不同医疗机构之间搜索加密数据。Xu等[17]利用授权机制、属性基加密机制和匹配机制，提出了一种基于区块链的隐私保护医疗数据分享方案，试图解决医疗领域的信息孤岛问题。

表1对以上提到的相关工作进行了比较。文献[14]和文献[15]都采用了代理重加密技术，使得用户端的解密计算相对轻量级，而本文方案引入了外包解

密机制降低用户解密的计算成本。文献[11]使用区块链智能合约为数据所有者（DO, data owner）建立了全局的加密搜索索引，但需要数据所有者和数据用户（DU, data user）之间进行实时交互，导致通信成本大幅增加。相反，文献[13]和文献[15-17]设计都不需要用户之间进行实时交互。此外，本文方案在实现安全搜索时也不需要用户之间的实时交互。

表1 基于区块链的医疗数据分享相关工作比较

方案	轻量级	安全搜索	DO与DU不需要实时交互
文献[11]	×	√	×
文献[13]	×	×	√
文献[14]	√	×	×
文献[15]	√	×	√
文献[16]	×	×	√
文献[17]	×	×	√
本文方案	√	√	√

1.2 可搜索加密

可搜索加密由Song等[2]首次提出。它允许在加密数据上进行直接搜索，为数据安全分享提供了便利。Boneh等[18]提出了一个基于公钥加密的关键字搜索（PEKS, public key encryption with keyword search）方案，该方案推动了可搜索加密的普及。因此，在数据分享中，SE在平衡隐私保护和可用性方面至关重要。接下来本文将讨论SE在医疗数据分享中的应用。

Zheng等[19]提出了一种可验证的属性基关键字搜索（VABKS, verifiable attribute-based keyword search）方案，允许授权用户搜索加密数据，将搜索操作外包给云，并对云的搜索操作进行验证。Chaudhari等[20]提出了一个接收者匿名的属性基公钥加密关键字搜索方案，它允许对存储在公共云上的加密数据进行安全的关键字搜索，同时实现了数据隐私保护、用户隐私保护和安全高效搜索。Gu等[21]提出了用于雾计算中分布式数据存储的属性基公钥加密关键字搜索方案，实现了细粒度访问控制并降低了用户的计算成本。

近年来，可搜索加密也被广泛应用于医疗领域。Sangeetha等[22]设计了一个在云服务器中高效检索EMR的多关键字可搜索属性基加密方案，此方案减少了数据存储的冗余，提高了搜索效率，并增强了数据分享的安全性。Xiang等[23]结合ABE和区块链的优势提出了一个可搜索属性基加密（SABE, searchable attribute-based encryption）框架。该框架能够保证数据机密性、支持细粒度访问控制并且支持策略隐藏，适用于医疗领域。Zhao等[24]提出了一种适用于COVID-19数据的加密方案，该方案在保护数据隐私性和安全性的同时能允许多用户协同搜索加密数据，为访问数据提供了灵活性。Gao等[25]提出了一种区块链辅助的细粒度访问控制可搜索加密方案，该方案旨在优化云端电子健康记录的分享过程，将繁重的计算任务转移到边缘服务器上，解决了物联网中与云边缘计算相关的效率和公平性挑战。Chen等[26]提出了一种针对电子医疗记录（EHR, electronic health record）的可验证且动态的可搜索加密方案。该方案不仅支持对搜索结果的公开验证，还实现了动态数据更新的功能。

上述相关工作皆致力于数据安全性和可搜索加密功能，但恶意服务器场景下的搜索安全性尚未得到保障。

2 预备知识

本节将介绍一些基础知识，包括区块链与智能合约、双线性映射、线性秘密共享方案（LSSS，linear secret sharing scherne）、访问树转换为LSSS矩阵、KP-ABE以及决策性n-双线性Diffle-Hellman（n-DBDH, n-decisional bilinear Diffie-Hellman）假设。

2.1 区块链与智能合约

区块链在2008年由于中本聪发明的比特币而广为人知[27]。区块链作为比特币中所有交易的账本存储结构，具有去中心化、透明性、匿名性、防篡改、可追溯等特点。

智能合约是一种运行在区块链上的计算机程序，它在区块链参与者达成共识后部署，并且能够在无任何第三方参与的情况下自动执行。由于智能合约具有开放性、透明性、安全性、可靠性等特点，用户可以通过智能合约在区块链上实现一些可信且复杂的操作。

2.2 双线性映射

给定2个阶为素数p的乘法群G_1和G_T，其中p是一个大素数，g是G_1的生成元。一个双线性映射$e{:}G_1 \times G_1 \rightarrow G_T$具有以下一些性质。

1) 双线性。对于任意$P,Q \in G_1$，$u,v \in Z_P$，有

$e\left(P^u,Q^v\right)=e\left(P,Q\right)^{uv}$。

2) 非退化性。存在$P,Q\in G_1$，使得$e\left(P,Q\right)\neq 1$。

3) 可计算性。对于任意$P,Q\in G_1$，$e\left(P,Q\right)$可以被高效地计算。

2.3　线性秘密共享方案

假设$P=\left\{P_1,P_2,P_3,\cdots,P_m\right\}$是一组参与者，$\boldsymbol{M}$是一个$m\times t$矩阵，$\boldsymbol{M}_i$表示矩阵的第$i$行，$\rho(\cdot)$表示一个将矩阵的每行映射到相应参与者的函数，矩阵访问结构为$A=(\boldsymbol{M},\rho)$，线性秘密共享方案的主要步骤如下。

1) 给定秘密值$s\in Z_P$，选择$y_2,y_3,\cdots,y_t\in Z_P$，然后定义一个向量$\boldsymbol{y}=\left(s,y_2,y_3,\cdots,y_t\right)$，则参与方$\rho(i)\left(i\in\left[1,m\right]\right)$的秘密值为$\lambda_i=\boldsymbol{M}\boldsymbol{y}$。

2) 假设$W\in A$是一个属性集合，首先定义$I=\{i\}_{\rho(i)\in W}$，然后生成一组常数$\left\{c_i\in Z_P\right\}_{i\in I}$使得等式$\sum_{i\in I}\boldsymbol{M}_i c_i=(1,0,\cdots,0)$成立，则秘密值可以通过$\sum_{i\in I}\lambda_i c_i=s$计算得到。

2.4　访问树转换为LSSS矩阵

Lewko等[28]提出了一种根据访问树构建LSSS矩阵的方法。在访问树中，非叶节点代表AND或OR门限，叶节点代表属性。图1详细展示了访问树（A AND B）AND（C OR D）转换为LSSS矩阵的过程。具体转换规则如下。

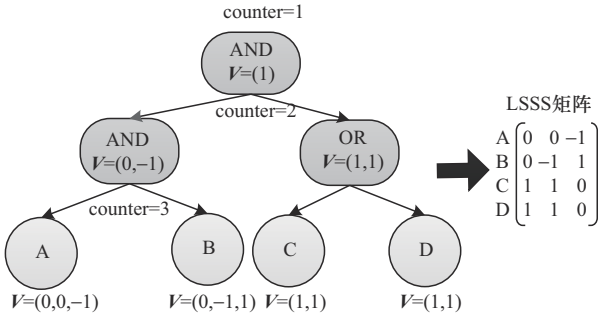


图1　访问树转换为LSSS矩阵的过程

1) 初始化。将访问树的根节点标注为一个长度为1的向量，具体为$\boldsymbol{V}=(1)$同时初始化一个全局变量counter = 1，然后对访问树进行广度优先遍历。

2) 如果父节点是一个被标记为向量$\boldsymbol{V}$的OR门限，则它的2个子节点也被标记为向量$\boldsymbol{V}$，并且保持counter不变。

3) 如果父节点是一个被标记为向量$\boldsymbol{V}$的AND门限，则按照以下规则对子节点进行标记。

① 将向量$\boldsymbol{V}$末尾用0填充，使向量$\boldsymbol{V}$的长度与当前的counter值一致。

② 右子节点被标记为$\left(\boldsymbol{V}\|1\right)$（||表示连接符）。

③ 左子节点被标记为$\left((0,\cdots,0)\|-1\right)$，其中0的数量等于counter值。

④ 随后，counter值加1，以容纳标签所表示的向量空间的扩展。

2.5　KP-ABE

ABE算法被分为2种类型，分别为密钥策略属性基加密（KP-ABE）[29]和密文策略属性基加密（CP-ABE）[30]。在KP-ABE方案中，用户的私钥与访问结构相关联，密文与属性集相关联，只有当属性集满足访问结构时，密文才能被成功解密。CP-ABE主要用于数据所有者对用户获取共享数据的权限进行限制，而KP-ABE主要服务于数据用户，使其能够按需获取满足其特定属性需求的数据。因此，在本文的应用场景中，KP-ABE更为适用，因为它能够确保医学研究机构仅获取满足其特定属性需求的EMR以进行研究。

KP-ABE方案的正式定义如下。

1) Setup$(\lambda)\rightarrow$(PP,MSK)。该算法将安全参数λ作为输入，输出公共参数PP和主密钥MSK。

2) KeyGen(PP,MSK,A)$\rightarrow$SK。该算法将公共参数PP、主密钥MSK和访问结构A作为输入，输出解密密钥SK。

3) Encrypt(PP,msg,attSet)$\rightarrow$CT。该算法将公共参数PP、明文消息msg和属性集合attSet作为输入，输出消息密文CT。

4) Decrypt(PP, CT, SK)$\rightarrow$msg/ $\perp$。该算法将公共参数PP、消息密文CT和解密密钥SK作为输入。如果attSet满足A，即属性集合满足访问结构，则算法将成功解密以获得明文消息msg。否则输出$\perp$，表示解密失败。

2.6　决策性n-双线性Diffie-Hellman假设

挑战者随机选择$a,s\in Z_P$，计算$2n+2$元组$\left(g,g^s,g^a,\cdots,g^{a^n},g^{a^{n+2}},\cdots,g^{a^{2n}}\right)$，其中$g$是乘法群$G_1$的生成元。如果没有概率多项式时间（PPT, probabilistic polynomial time）敌手能以不可忽略的优势区

分元组$\left(g,g^{s},g^{a},\cdots,g^{a^{n}},g^{a^{n+2}},\cdots,g^{a^{2n}},e\left(g^{a^{n+1}},g^{s}\right)\right)$和$\left(g,g^{s},g^{a},\cdots,g^{a^{n}},g^{a^{n+2}},\cdots,g^{a^{2n}},Y\right)$，其中$Y$表示$G_T$中的一个随机数，那么n-DBDH假设成立。本文方案的安全性依赖于n-DBDH假设。

3　系统模型

本节将从3个方面介绍本文方案，包括系统架构、方案框架和安全模型。

3.1　系统架构

系统模型架构由6个实体组成，分别为医院、医学研究机构（MRI）、云服务器、区块链、智能合约和可信机构（TA, trusted authority），系统模型如图2所示。

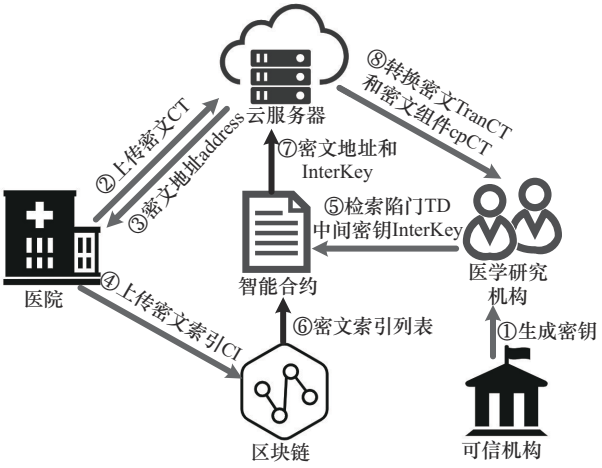


图2　系统模型

1) 医院。医疗数据所有者，负责对医疗隐私数据进行加密，将密文上传到云服务器进行存储，并将密文存储地址发布到区块链上。

2) 医学研究机构。医疗数据的使用者，主要负责生成数据检索陷门，向智能合约发出数据查询请求，检验云服务器是否篡改密文以及进行最后的数据解密。

3) 云服务器。不可信实体，一方面是指对隐私数据的好奇；另一方面，为节省计算资源，可能不会提供正确且完整的数据查询结果。云服务器一般负责存储医疗数据密文和执行预解密计算。

4) 智能合约。本文涉及一个数据检索智能合约（RetrSC, retrieval smart contract），主要负责检索满足MRI特定属性需求的医疗数据，并将该医疗数据地址告知云服务器。

5) 区块链。主要负责存储密文索引以及将智能合约RetrSC部署到区块链上。

6) 可信机构。完全可信的实体，主要负责系统初始化和生成密钥。

3.2　方案框架

方案框架主要由8个算法组成。

1) $\text{Setup}(\lambda)\rightarrow(\text{PP},\text{MSK})$。该算法将安全参数$\lambda$作为输入，输出公共参数PP和主密钥MSK。

2) $\text{ACSKG}(\text{PP},\text{MSK},(\boldsymbol{M},\rho))\rightarrow \text{ACSK}_{(\boldsymbol{M},\rho)}$。该算法输入公共参数PP、主密钥MSK和LSSS访问控制结构$(\boldsymbol{M},\rho)$，输出访问控制密钥$\text{ACSK}_{(\boldsymbol{M},\rho)}$。

3) $\text{TrapKGen}\left(\text{PP},\text{MSK},\text{ACSK}_{(\boldsymbol{M},\rho)}\right)\rightarrow(\text{DeKey},\text{InterKey})$。该算法将公共参数PP、主密钥MSK和访问控制密钥$\text{ACSK}_{(\boldsymbol{M},\rho)}$作为输入，输出MRI的最终解密密钥DeKey和用于云端进行预解密的中间密钥InterKey。

4) $\text{MEnc}(\text{PP},\text{msg},\text{attSet},\text{kwd})\rightarrow(\text{CT},\text{CI})$。该算法将明文消息msg、公共参数PP、属性集合attSet以及与明文对应的关键字kwd作为输入，输出明文数据的密文CT和密文索引CI。

5) $\text{TrapdoorGen}(\text{PP},\text{Sekeyword})\rightarrow \text{TD}_{\text{Sekeyword}}$。该算法将公共参数PP和检索关键字Sekeyword作为输入，输出检索陷门$\text{TD}_{\text{Sekeyword}}$。

6) $\text{Search}\left(\text{PP},\text{TD}_{\text{Sekeyword}},\text{CI}\right)\rightarrow \text{address}/\perp$。该算法将公共参数PP、检索陷门$\text{TD}_{\text{Sekeyword}}$和密文索引CI作为输入。如果存在与$\text{TD}_{\text{Sekeyword}}$匹配的数据，它将输出匹配数据的地址address。否则，将输出$\perp$。

7) $\text{InterDe}(\text{CT},\text{InterKey})\rightarrow \text{TranCT},\text{cpCT}/\perp$。该算法将密文CT和中间密钥InterKey作为输入，如果与密文CT相关联的属性集合符合InterKey相关联的访问结构，该算法将输出转换密文TranCT和密文组件cpCT。否则，将输出$\perp$。

8) $\text{Decrypt}(\text{TranCT},\text{cpCT},\text{DeKey})\rightarrow \text{msg}$。该算法使用解密密钥DeKey对转换密文TranCT和密文组件cpCT进行最终解密，恢复出明文消息msg。

3.3　安全模型

在安全模型中，本文考虑了2种常见的攻击类型，分别为选择明文攻击（CPA）和关键字猜测攻击（KGA）。

1) 选择明文攻击。对于CPA，安全模型有挑战者$\mathcal{C}$和敌手$\mathcal{A}$这2个角色。安全模型的定义如下。

初始化。敌手$\mathcal{A}$宣布挑战的属性集合attSet。

设置。挑战者$\mathcal{C}$选择安全参数λ并运行Setup算法生成公共参数PP和主密钥MSK。然后挑战者$\mathcal{C}$将公共参数PP传递给敌手$\mathcal{A}$。

阶段1。敌手$\mathcal{A}$发出关于LSSS结构$(\boldsymbol{M},\rho)$的密钥查询请求。挑战者$\mathcal{C}$执行访问控制密钥生成算法$\mathrm{ACSKG}(\mathrm{PP},\mathrm{MSK},(\boldsymbol{M},\rho))$和中间密钥生成算法$\mathrm{TrapKGen}\left(\mathrm{PP},\mathrm{MSK},\mathrm{ACSK}_{(\boldsymbol{M},\rho)}\right)$生成访问控制密钥$\mathrm{ACSK}_{(\boldsymbol{M},\rho)}$、最终解密密钥DeKey和中间密钥InterKey，并将密钥返回给敌手$\mathcal{A}$。

挑战。敌手$\mathcal{A}$选择一对长度相同的明文消息msg_0和msg_1，以及关键字kwd，并发送给挑战者$\mathcal{C}$。挑战者$\mathcal{C}$随机选择一个明文消息msg_x，其中$x\in\{0,1\}$，并执行加密算法$\mathrm{MEnc}(\mathrm{PP},\mathrm{msg},\mathrm{attSet},\mathrm{kwd})$，将$\mathrm{msg}_x$与目标属性集合attSet加密，然后将密文CT发送给敌手$\mathcal{A}$。

阶段2。敌手$\mathcal{A}$重复阶段1的工作，并继续向挑战者$\mathcal{C}$请求密钥。

猜测。敌手$\mathcal{A}$猜测挑战阶段由挑战者$\mathcal{C}$发送的密文。如果估计值$x'=x$，则敌手$\mathcal{A}$获胜。

假设敌手$\mathcal{A}$获胜的概率是$\Pr[x'=x]$，则敌手$\mathcal{A}$的优势为$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{CPA}}=\left|\Pr[x'=x]-\frac{1}{2}\right|$。然后给出基于CPA的方案安全定义，如定义1所示。

定义1　（基于CPA的方案安全）若所有的概率多项式时间算法$\mathcal{A}$在上述实验中的优势$\mathrm{Adv}_{\mathcal{A}}$是可忽略的，则称本文方案在CPA下是安全的。

2) 关键字猜测攻击。为保证数据的相关信息无法根据加密关键字或检索陷门被猜测，需要保证数据索引和检索陷门不会导致关键字明文信息泄露。因此，本文考虑了KGA。安全模型的定义如下。

初始化。挑战者$\mathcal{C}$选择安全参数λ并运行算法Setup生成公共参数PP和主密钥MSK。公共参数PP被传递给敌手$\mathcal{A}$。

查询。敌手$\mathcal{A}$反复向挑战者$\mathcal{C}$提交检索关键字Sekeyword以获取搜索关键字陷门。挑战者$\mathcal{C}$执行$\mathrm{TrapdoorGen}(\mathrm{PP},\mathrm{Sekeyword})\rightarrow\mathrm{TD}_{\mathrm{Sekeyword}}$算法，并将检索陷门$\mathrm{TD}_{\mathrm{Sekeyword}}$返回给敌手$\mathcal{A}$。

挑战。敌手$\mathcal{A}$选择2个长度相同的关键字K_0和K_1，且这2个关键字在上述查询阶段没有被查询过，并将它们发送给挑战者$\mathcal{C}$。挑战者$\mathcal{C}$随机选择一个关键字K_y，其中$y\in\{0,1\}$，通过执行陷门生成算法$\mathrm{TrapdoorGen}(\mathrm{PP},K_y)\rightarrow\mathrm{TD}_{K_y}$生成一个关键字陷门，并将其发送给敌手$\mathcal{A}$。

猜测。在查询了N个不同的关键字后，敌手猜测挑战阶段由挑战者$\mathcal{C}$发送的关键字。如果估计值$y'=y$，则敌手$\mathcal{A}$获胜。即如果能够正确猜测，则敌手$\mathcal{A}$获胜。

假设敌手$\mathcal{A}$获胜的概率是$\Pr[y'=y]$，则敌手$\mathcal{A}$的优势为$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{KGA}}=\left|\Pr[y'=y]-\frac{1}{2}\right|$。然后给出基于KGA的方案安全定义，如定义2所示。

定义2　（基于KGA的方案安全）若所有的概率多项式时间算法$\mathcal{A}$在上述实验中的优势$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{KGA}}$是可忽略的，则称本文方案在KGA下是安全的。

4　具体实施

本节列举了一个应用示例描述本文方案的具体流程，同时介绍了各个算法的具体实现步骤，系统主要参数如表2所示。

表2　**系统主要参数**

参数	含义
λ	安全参数
PP	公共参数
MSK	主密钥
$(\boldsymbol{M},\rho)$	访问结构
$\mathrm{ACSK}_{(\boldsymbol{M},\rho)}$	访问控制密钥,与访问结构$(\boldsymbol{M},\rho)$关联
InterKey	中间密钥,用于云服务器进行预解密
DeKey	解密密钥,用于用户进行最终解密
msg	医疗明文数据
ATT	系统属性域
attSet	医疗数据的属性集合
kwd	与医疗数据绑定的关键字
Sekeyword	数据检索请求中的关键字
CT	密文
CI	密文索引
TranCT	转换密文
cpCT	密文组件$\mathrm{cpCT}=\{\mathrm{CT}_1,H\}$

4.1　应用举例

由于医疗数据包含患者的敏感信息，所以医院需要对医疗数据进行加密。此外，MRI对数据有特定属性需求，并不需要获取所有的医疗数据，因此有必要根据MRI的特定属性需求分配访问结构。

假设系统属性空间为{男性，女性，青年，中年，老年}。医院有3份医疗记录，如表3所示。

表3　　医疗记录

医疗数据	属性	数据关键字
Rec_1	女性,青年	糖尿病
Rec_2	男性,青年	肺炎
Rec_3	女性,中年	肺炎

医院对这3份医疗记录进行加密，并将密文存储在云服务器中，然后将每份医疗数据的密文地址与相应的数据关键字组合生成数据索引集，并将数据索引集存储到区块链。

假设MRI的数据访问需求旨在检索青年女性或中年女性的肺炎患者数据，其需求访问结构定义为“（青年OR中年）AND女性”，搜索的数据关键字为“肺炎”。TA根据{（青年OR中年）AND女性}为MRI定义一个LSSS访问结构。LSSS矩阵生成过程如图3所示。

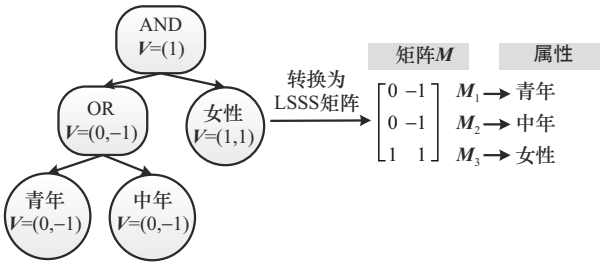


图3　LSSS矩阵生成过程

根据访问结构（访问树），TA将生成一个3×2的矩阵$\boldsymbol{M}_{3\times 2}$，则LSSS的访问结构是$\left(\boldsymbol{M}_{3\times 2},\rho\right)$，其中$\rho$是一个映射函数，具体表示为将矩阵$\boldsymbol{M}_{3\times 2}$的每一行$\left\{\boldsymbol{M}_k\right\}_{k\in\{1,3\}}$分别映射到“青年”“中年”和“女性”属性上。TA为每个属性计算一个秘密值切片$\lambda_{\rho(k)}$，并根据每个属性值和属性的秘密值切片计算生成访问控制密钥$\mathrm{ACSK}_{(\boldsymbol{M},\rho)}$，最终得到解密密钥DeKey和中间密钥InterKey。然后，TA将InterKey和DeKey发送给MRI。MRI将根据数据需求的关键字生成搜索关键字陷门，并上传搜索关键字陷门和中间密钥InterKey到智能合约。

数据需求满足过程如图4所示，智能合约通过自动匹配加密数据索引与搜索关键字，成功识别出Rec_2和Rec_3记录满足MRI的搜索条件，因此，智能合约将Rec_2和Rec_3的数据存储地址和MRI的中间密钥InterKey发送给云服务器。

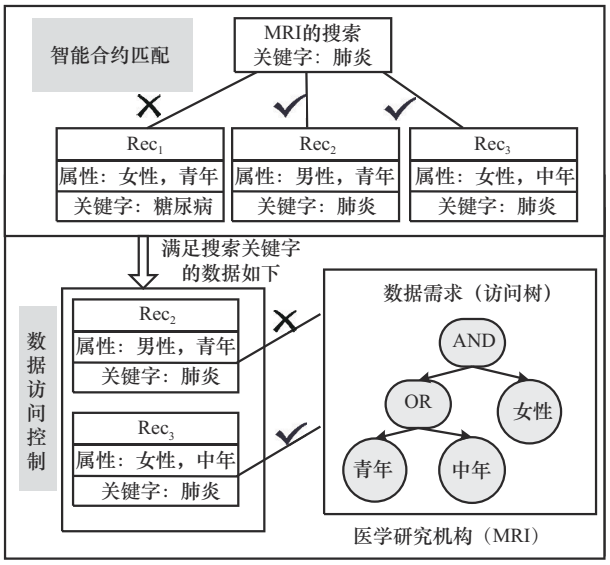


图4　数据需求满足过程

然而，从图4可以看出，只有Rec_3的属性值满足LSSS访问结构，因此云服务器只能对Rec_3进行预解密，然后将预解密结果TranCT发送给MRI。最后，MRI使用解密密钥DeKey进行最终解密，以获取数据明文。

4.2　具体实现

1) 系统初始化

在初始化阶段，TA设置一个安全参数λ，执行算法$\mathrm{Setup}(\lambda)\rightarrow(\mathrm{PP},\mathrm{MSK})$生成系统公共参数PP和主密钥MSK。首先，TA选择2个阶为素数p的乘法群G_1和G_T，其中g为G_1的生成元。选择双线性映射$e{:}G_1\times G_1\rightarrow G_T$，定义2个抗碰撞哈希函数如式(1)和式(2)所示，并随机选择$a,b\in Z_P$和$g_1,T_0\in G_1$，然后通过式(3)计算Y。

$$H_1{:}\{0,1\}^*\rightarrow G_1 \tag{1}$$

$$H_2{:}\{0,1\}^*\times\{0,1\}^k\rightarrow\{0,1\}^1 \tag{2}$$

$$Y=e\left(g,g\right)^a \tag{3}$$

TA定义系统属性域$\mathrm{ATT}=\left\{\mathrm{att}_1,\mathrm{att}_2,\cdots,\mathrm{att}_n\right\}$，

对于每个属性 $\mathrm{att}_i \in \mathrm{ATT}$，TA 随机选择 $t_{\mathrm{att}_i} \in G_1$。公共参数 PP 和主密钥 MSK 如式(4)和式(5)所示，其中 PP 公开发布，MSK 由 TA 秘密保存。

$$\mathrm{PP} = \begin{Bmatrix} G_1,G_T,g,g_1,b,e,p,Y, \\ H_1,H_2,T_0,\{t_{\mathrm{att}_i}\}_{\mathrm{att}_i \in \mathrm{ATT}} \end{Bmatrix} \tag{4}$$

$$\mathrm{MSK} = a \tag{5}$$

2) 访问控制密钥生成

MRI 发送一个数据请求，其中包含 MRI 对数据属性和数据关键字的需求，然后 TA 根据请求为 MRI 定义一个 LSSS 访问结构 $(\boldsymbol{M},\rho)$，其中 $\boldsymbol{M}$ 是一个 f 行 m 列的矩阵，f 是数据请求中属性的数量，$\boldsymbol{M}_k$ 表示矩阵的第 k 行，ρ 是将矩阵 $\boldsymbol{M}$ 的每一行 $\{\boldsymbol{M}_k\}_{k\in\{1,f\}}$ 映射到一个属性的函数，即 $\rho(k)$ 表示矩阵 $\boldsymbol{M}$ 第 k 行代表的属性，而 $t_{\rho(k)}$ 表示属性 $\rho(k)$ 所对应的值。

TA 执行算法 $\mathrm{ACSKG}(\mathrm{PP},\mathrm{MSK},(\boldsymbol{M},\rho))$ 生成访问控制密钥 $\mathrm{ACSK}_{(\boldsymbol{M},\rho)}$。首先，TA 计算向量 $\boldsymbol{y} = (a,y_2,y_3,\cdots,y_m)$，使其满足 $\boldsymbol{y}(1,0,\cdots,0) = a$，然后计算秘密值分片 $\lambda_{\rho(k)} = \boldsymbol{M}_k\boldsymbol{y}$。其次，对于每个 $k \in \{1,f\}$，TA 随机选择 $c_k \in Z_P$，最后计算如式(9)所示的访问控制密钥 $\mathrm{ACSK}_{(\boldsymbol{M},\rho)}$，并将访问控制密钥 $\mathrm{ACSK}_{(\boldsymbol{M},\rho)}$ 发送给 MRI。

$$A_{1,k} = g^{\lambda_{\rho(k)}}\left(T_0 t_{\rho(k)}\right)^{c_k} \tag{6}$$

$$A_{2,k} = g^{c_k} \tag{7}$$

$$A_{3,k,i} = \left\{t_{\mathrm{att}_i}^{c_k}\right\}_{\mathrm{att}_i \in \mathrm{ATT}\setminus\{\rho(k)\}} \tag{8}$$

$$\mathrm{ACSK}_{(\boldsymbol{M},\rho)} = \left\{(\boldsymbol{M},\rho),\left\{A_{1,k},A_{2,k},\left\{A_{3,k,i}\right\}_{\mathrm{att}_i \in \mathrm{ATT}\setminus\{\rho(k)\}}\right\}_{k\in[1,f]}\right\} \tag{9}$$

3) 最终解密密钥和中间密钥生成

TA 执行 $\mathrm{TrapKGen}\left(\mathrm{PP},\mathrm{MSK},\mathrm{ACSK}_{(\boldsymbol{M},\rho)}\right)$ 算法生成解密密钥 DeKey 和中间密钥 InterKey。在此算法中，TA 随机选择 $d \in Z_P$ 作为解密密钥 DeKey，然后计算中间密钥 InterKey。最后 TA 将式(13)和式(14)所示解密密钥 DeKey 和中间密钥 InterKey 传输给 MRI。

$$A_{1,k}' = A_{1,k}{}^{d} = g^{\lambda_{\rho(k)}}(T_0 t_{\rho(k)})^{dc_k} \tag{10}$$

$$A_{2,k}' = A_{2,k}{}^{d} = g^{dc_k} \tag{11}$$

$$\left\{A_{3,k,i}' = A_{3,k,i}{}^{d} = t_{\mathrm{att}_i}{}^{dc_k}\right\}_{\mathrm{att}_i \in \mathrm{ATT}\setminus\{\rho(k)\}} \tag{12}$$

$$\mathrm{Dekey} = d \tag{13}$$

$$\mathrm{InterKey} = \left\{(\boldsymbol{M},\rho),\left\{A_{1,k}',A_{2,k}',\left\{A_{3,k,i}'\right\}_{\mathrm{att}_i \in \mathrm{ATT}\setminus\{\rho(k)\}}\right\}_{k\in[1,f]}\right\} \tag{14}$$

4) 明文加密

医院执行 $\mathrm{MEnc}(\mathrm{PP},\mathrm{msg},\mathrm{attSet},\mathrm{kwd})$ 加密算法加密医疗数据明文消息 msg 和关键字 kwd。首先随机选择 $s \in Z_P$，计算密文 CT。

$$\mathrm{CT}_1 = \mathrm{msg}Y^s \tag{15}$$

$$\mathrm{CT}_2 = g^s \tag{16}$$

$$\mathrm{CT}_3 = \left(T_0 \prod_{\mathrm{att}_i \in \mathrm{attSet}} t_{\mathrm{att}_i}\right)^s \tag{17}$$

$$H = H_2(\mathrm{CT}_1,\mathrm{kwd}) \tag{18}$$

$$\mathrm{CT} = \{\mathrm{attSet},\mathrm{CT}_1,\mathrm{CT}_2,\mathrm{CT}_3,H\} \tag{19}$$

然后，医院将密文 CT 上传到云服务器进行存储，并获取存储地址 address。随后，医院随机选择 $r \in Z_P$，计算密文索引 CI。

$$I_1 = e(g_1,g)^{br} \tag{20}$$

$$I_2 = g^r \tag{21}$$

$$I_3 = H_1(\mathrm{kwd})^r \tag{22}$$

$$\mathrm{CI} = \{I_1,I_2,I_3,\mathrm{address}\} \tag{23}$$

密文索引 CI 被上传到区块链进行存储。加密阶段数据流如图 5 所示。

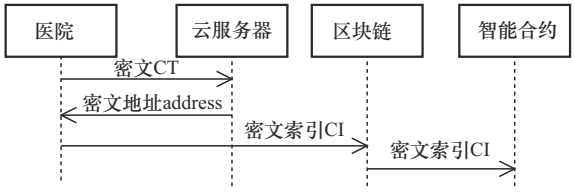


图 5　加密阶段数据流

5) 陷门生成

MRI 执行 TrapdoorGen(PP, Sekeyword) 算法生成与搜索关键字 Sekeyword 相对应的检索陷门 $\mathrm{TD}_{\mathrm{Sekeyword}}$ 该算法随机选择 $r_1 \in Z_P$，然后计算 $\mathrm{TD}_{\mathrm{Sekeyword}}$。

$$\mathrm{TD}_1 = g_1^b H_1(\mathrm{Sekeyword})^{r_1} \tag{24}$$

$$\mathrm{TD}_2 = g^{r_1} \tag{25}$$

$$\mathrm{TD}_{\mathrm{Sekeyword}}=\left\{\mathrm{TD}_1,\mathrm{TD}_2\right\} \tag{26}$$

随后，检索陷门$\mathrm{TD}_{\mathrm{Sekeyword}}$发送到智能合约。

6) 搜索

当智能合约接收到检索陷门$\mathrm{TD}_{\mathrm{Sekeyword}}$时，自动执行$\mathrm{Search}\left(\mathrm{PP},\mathrm{TD}_{\mathrm{Sekeyword}},\mathrm{CI}\right)\rightarrow \mathrm{address}/\perp$算法获取匹配数据的存储地址。此算法依次检查密文索引CI是否满足式(27)。若等式成立，则表示相关数据满足MRI的关键字查询需求，智能合约将发送相应的存储地址给云服务器。否则，输出⊥。

$$e\left(\mathrm{TD}_2,I_3\right)I_1=e\left(\mathrm{TD}_1,I_2\right) \tag{27}$$

考虑到云服务器是不完全可信实体，在数据搜索时存在潜在的欺诈风险，如仅检索部分数据来减少计算开销等。因此，本文引入智能合约完成检索过程，避免第三方的欺诈行为。数据检索智能合约（RetrSC）如算法1所示。

算法1 数据检索智能合约

给定公共参数PP，检索陷门$\mathrm{TD}=\left(\mathrm{TD}_1,\mathrm{TD}_2\right)$，以及密文索引CI的列表List〈CI〉，其中密文索引$\mathrm{CI}=\left\{I_1,I_1,I_3,\mathrm{address}\right\}$，此算法输出与检索陷门TD匹配数据的地址列表List〈address〉。

① 初始化 List〈address〉= NULL

② for each CI ∈ List〈CI〉do

③ 计算$E_1=e\left(\mathrm{TD}_1,I_3\right)$

⑤ 计算$\mathrm{key}_1=E_1I_1$

⑤ 计算$\mathrm{key}_2=e\left(\mathrm{TD}_1,I_2\right)$

⑥ if $\mathrm{key}_1=\mathrm{key}_2$ then

⑦ 添加CI.address到List〈address〉

⑧ end if

⑨ end for

⑩ return List〈address〉

7) 中间解密

云服务器执行$\mathrm{InterDe}\left(\mathrm{CT},\mathrm{InterKey}\right)$算法对密文CT进行预解密。首先，云服务器检查医疗数据的属性集是否满足LSSS访问结构。如果不满足，则输出⊥，否则，构造一组常量$\left\{v_k\right\}\in Z_p$，使得$\sum_{k\in\Omega}\boldsymbol{M}_kv_k=(1,0,\cdots,0)$成立，然后根据式(28)计算TranCT，其中$\Omega$代表满足$\rho_{(k)}\in\mathrm{attSet}$的所有$k$的集合。最后，将转换后的密文TranCT和密文组件$\mathrm{cpCT}=\left\{\mathrm{CH}_1,H\right\}\in\mathrm{CT}$发送给MRI。

$$\mathrm{TranCT}=\frac{e\left(\mathrm{CT}_3,\prod_{k\in\Omega}\left(A_{2,k}{}'\right)^{v_k}\right)}{e\left(\mathrm{CT}_2,\prod_{k\in\Omega}\left(A_{1,k}{}'\prod_{\mathrm{att}_i\in\mathrm{attSet}\backslash\{\rho(k)\}}A_{3,k,i}{}'\right)^{v_k}\right)} \tag{28}$$

8) 解密

获得转换后的密文TranCT和密文组件cpCT后，MRI首先检查密文数据是否有效。MRI使用其需求数据关键字Sekeyword和cpCT中的CT_1计算$H'=H_2(\mathrm{CT}_1,\mathrm{Sekeyword})$。如果$H'=H$，则$\mathrm{CT}_1$未被篡改，该数据具有研究价值。然后MRI通过式(29)来恢复明文消息msg。

$$\mathrm{msg}=\mathrm{CT}_1\mathrm{TranCT}^{\frac{1}{d}} \tag{29}$$

5 方案分析

本节将对本文方案进行详细的分析，重点关注安全性和性能2个关键维度。通过综合评估，旨在验证本文方案的正确性，并突显其效率。

5.1 正确性分析

本节涵盖了2个方面的正确性证明：解密正确性和密文检索正确性。

1) 解密正确性证明。当与检索关键词匹配的医疗数据密文的属性满足MRI的访问结构时，云服务器将对密文进行预解密，并将得到的转换密文TranCT转发给MRI，MRI将通过式(30)恢复医疗数据明文。相反，如果医疗数据的密文属性不满足MRI的访问结构，那么秘密值a无法被恢复，因此云服务器将无法进行预解密，从而无法获得TranCT。自然也意味着MRI无法恢复医疗数据的明文。

$$\mathrm{CT}_1\mathrm{TranCT}^{\frac{1}{d}}=\mathrm{msg} \tag{30}$$

式(30)的详细计算过程见附录1，其详细计算过程证明了解密的正确性。

2) 密文检索正确性证明。在搜索过程中，MRI将其检索陷门$\mathrm{TD}_{\mathrm{Sekeyword}}=\left\{\mathrm{TD}_1,\mathrm{TD}_2\right\}$提供给智能合约RetrSC。RetrSC依次遍历所有的数据索引，并针对每一个索引检查式(31)是否成立，若式(31)成立，则表明kwd = Sekeyword，即当前数据满足MRI的检索需求，其地址将被添加到地址列表List〈address〉中。若List〈address〉为空，则表示没有与Sekeyword匹配的数据。

$$e\left(\mathrm{TD}_2,I_3\right)I_1=e\left(\mathrm{TD}_1,I_2\right) \tag{31}$$

式(31)的正确性证明见附录2。

5.2　安全性分析

本节将通过证明定理1和定理2来证明本文方案能够抵抗CPA和KGA。

定理1　在n-DBDH假设下，本文方案能够抵抗CPA。

证明　假设存在一个PPT攻击者$\mathcal{A}$在本文方案中以不可忽略优势赢得CPA的安全挑战，那么存在另一个PPT攻击者$\mathcal{C}$，可通过以下游戏以不可忽略的优势解决n-DBDH假设问题。

选择双线性映射$e{:}G_1\times G_1\rightarrow G_T$，其中$G_1$和$G_T$是以素数$n$为阶的乘法群，$g$为$G_1$的生成元。挑战者$\mathcal{C}$随机选择$s,a\in Z_P$，$R\in G_T$，$\eta\in\{0,1\}$，同时生成$2n+1$元组$\left(g,g^s,g^a,\cdots,g^{a^n},g^{a^{n+2}},\cdots,g^{a^{2n}},T\right)$，如果$\eta=1$，则表明$T=e\left(g^{a^{n+1}},g^s\right)$，否则$T=R$。

初始化。敌手$\mathcal{A}$宣布挑战的属性集合attSet。

设置。挑战者$\mathcal{C}$选择安全参数λ并运行Setup(λ)算法。首先，挑战者$\mathcal{C}$随机选择$a'\in\mathbb{Z}_p$，使得$Y=e\left(g,g\right)^a=e\left(g,g\right)^{a'}e\left(g^a,g^{a^n}\right)$成立，即满足$a=a'+a^{n+1}$。随后挑战者$\mathcal{C}$对每个属性$\mathrm{att}_i\in\mathrm{ATT}$随机选择$\{t_{\mathrm{att}_i}\}\in\mathbb{Z}_p$，并选择$T_0\in G_1$。最后，挑战者$\mathcal{C}$秘密保存MSK$=\{a,a'\}$，并将公共参数PP$=\left\{G_1,G_T,g,e,T_0,\left\{t_{\mathrm{att}_i}\right\}_{i\in[1,n]}\right\}$传给敌手$\mathcal{A}$。

阶段1。敌手$\mathcal{A}$向挑战者$\mathcal{C}$发出一系列查询，挑战者$\mathcal{C}$通过以下方式响应攻击者的查询。

访问控制密钥请求。假设存在一个LSSS访问结构$(\boldsymbol{M},\rho)$，使攻击者的目标属性集合attSet不满足该访问结构。挑战者$\mathcal{C}$生成一个向量$\boldsymbol{v}$，使其满足$\boldsymbol{v}(1,0,\cdots,0)=a$，并计算$\lambda_{\rho(k)}=\boldsymbol{M}_k\boldsymbol{v}$。随后挑战者$\mathcal{C}$随机选择$r_k\in Z_p$，计算$A_{1,k}=g^{\lambda_{\rho_{(k)}}}\left(T_0t_{\rho(k)}\right)^{r_k}$、$A_{2,k}=g^{r_k}$和$\left\{A_{3,k,i}=t_{\mathrm{att}_i}^{r_k}\right\}_{\mathrm{att}_i\in\mathrm{ATT}\backslash\rho(k)}$。然后挑战者$\mathcal{C}$将访问控制密钥$\mathrm{ACSK}_{(\boldsymbol{M},\rho)}$转发给敌手$\mathcal{A}$。

中间密钥请求。敌手$\mathcal{A}$向挑战者$\mathcal{C}$询问基于LSSS访问结构$(\boldsymbol{M},\rho)$的中间密钥InterKey和解密密钥DeKey。挑战者$\mathcal{C}$随机选择$d\in Z_p$并计算$A_{1,k}{}'=A_{1,k}{}^d=g^{d\lambda_{\rho(k)}}\left(T_0t_{\rho(k)}\right)^{dr_k}$、$A_{2,k}{}'=A_{2,k}{}^d=g^{dr_k}$和$\left\{A_{3,k,i}{}'=t_{\mathrm{att}_i}{}^{dr_k}\right\}_{\mathrm{att}_i\in\mathrm{ATT}\backslash\rho(k)}$，然后将式(32)中的中间密钥InterKey和解密密钥DeKey$=d$发送给敌手$\mathcal{A}$。

$$\mathrm{InterKey}=\left\{(\boldsymbol{M},\rho),\left\{A_{1,k}{}',A_{2,k}{}',\left\{A_{3,k,i}{}'\right\}_{\mathrm{att}_i\in\mathrm{ATT}\backslash\{\rho(k)\}}\right\}_{k\in[1,f]}\right\} \tag{32}$$

挑战。敌手$\mathcal{A}$选择一对长度相同的明文数据M_0和M_1以及关键字kwd，并发送给挑战者$\mathcal{C}$。挑战者$\mathcal{C}$随机选择一个明文M_x，其中$x\in\{0,1\}$。随后挑战者$\mathcal{C}$计算$\mathrm{CT}_1=M_xTe\left(g^s,g^{a'}\right)$、$\mathrm{CT}_2=g^s$和$\mathrm{CT}_3=\left(T_0\prod_{\mathrm{att}_i\in\mathrm{attSet}}t_{\mathrm{att}_i}\right)^s$，然后将式(33)中的密文CT转发给敌手$\mathcal{A}$。

$$\mathrm{CT}=\left\{\mathrm{attSet},\mathrm{CT}_1,\mathrm{CT}_2,\mathrm{CT}_3\right\} \tag{33}$$

阶段2。敌手$\mathcal{A}$重复阶段1的工作，并继续向挑战者$\mathcal{C}$请求密钥。

猜测。敌手$\mathcal{A}$返回对M_x的猜测结果。如果$x'=x$，则挑战者$\mathcal{C}$输出$\eta=1$以表示$T=e\left(g^{a^{n+1}},g^s\right)$，否则输出$\eta=0$以表示$T$为随机数。

如果$T=e\left(g^{a^{n+1}},g^s\right)$，则存在式(34)成立。

$$\begin{aligned}&\mathrm{CT}_1=M_xTe\left(g^s,g^{a'}\right)=\\&M_xe\left(g^{a^{n+1}},g^s\right)e\left(g^s,g^{a'}\right)=\\&M_xe\left(g,g^{as}\right)\end{aligned} \tag{34}$$

即密文CT$=\left\{\mathrm{attSet},\mathrm{CT}_1,\mathrm{CT}_2,\mathrm{CT}_3\right\}$可用。若敌手$\mathcal{A}$的优势为$\mathrm{Adv}_{\mathcal{A}}=\varepsilon$，则挑战者$\mathcal{C}$获胜的优势为

$$\Pr\left[(x'=x)|\eta=1\right]=\varepsilon+\frac{1}{2} \tag{35}$$

如果T是一个随机数，那么挑战者$\mathcal{C}$获胜的优势为

$$\Pr\left[(x'\neq x)|\eta=0\right]=\Pr\left[(x'=x)|\eta=0\right]=\frac{1}{2} \tag{36}$$

因此，挑战者$\mathcal{C}$在打破n-DBDH假设中的优势如式(37)所示。

$$\begin{aligned}&\mathrm{Adv}_{\mathcal{C}}=\frac{1}{2}\left\{\left|\Pr\left[(x'=x)|\eta=1\right]\right|+\right.\\&\left.\left|\Pr\left[(x'\neq x)|\eta=0\right]\right|\right\}-\frac{1}{2}=\\&\frac{1}{2}\left(\varepsilon+\frac{1}{2}+\frac{1}{2}\right)-\frac{1}{2}=\frac{1}{2}\varepsilon\end{aligned} \tag{37}$$

综上所述，若敌手$\mathcal{A}$打破本文方案的优势为ε，则挑战者$\mathcal{C}$打破n-DBDH假设的优势为$\frac{1}{2}\varepsilon$。如果ε是不可忽略的，那么挑战者$\mathcal{C}$在多项式时间内解决n-DBDH问题的优势也是不可忽略的，这显然是错误的。因此，没有任何PPT攻击者能以不可忽略的优势赢得本文方案中的游戏。因此，本文方案被证明在n-DBDH假设下是CPA安全的。证毕。

定理2 在随机预言模型下，本文方案能够抵抗KGA。

证明 假设存在一个试图打破KGA的敌手$\mathcal{A}$。挑战者$\mathcal{C}$与敌手$\mathcal{A}$进行安全游戏，敌手$\mathcal{A}$赢得安全游戏的前提是正确区分$H_1(K_0)^{r_0}$和$H_1(K_1)^{r_1}$。

初始化。敌手$\mathcal{A}$选择目标属性集合attSet。挑战者$\mathcal{C}$选择安全参数λ并执行Setup(λ)算法。挑战者$\mathcal{C}$随机选择$a',a\in\mathbb{Z}_p$，使其满足$a=a'+a^{n+1}$，即等式$Y=e(g,g)^{a}=e(g,g)^{a'}e\left(g^{a},g^{a^{n}}\right)$成立。挑战者$\mathcal{C}$对每个属性$\text{att}_i\in\text{ATT}$随机选择$\{t_{\text{att}_i}\}\in\mathbb{Z}_p$，并选择$b\in\mathbb{Z}_p$以及$T_0,g_1\in G_1$。然后选择一个抗碰撞哈希函数$H_1:\{0,1\}^{*}\rightarrow G_1$。最后，挑战者$\mathcal{C}$将公共参数$PP=\left\{G_1,G_T,g,g_1,b,e,H_1,T_0,\left\{t_{\text{att}_i}\right\}_{i\in[1,n]}\right\}$转发给敌手$\mathcal{A}$，主密钥$\text{MSK}=\{a,a'\}$由挑战者$\mathcal{C}$秘密保存。

查询。敌手$\mathcal{A}$反复向挑战者$\mathcal{C}$提交Sekeyword来获取搜索关键字陷门。挑战者$\mathcal{C}$执行算法TrapdoorGen$(\text{PP},\text{Sekeyword})\rightarrow\text{TD}_{\text{Sekeyword}}$，并将$\text{TD}_{\text{Sekeyword}}$返回给敌手$\mathcal{A}$。

挑战。敌手$\mathcal{A}$选择2个具有相同长度的关键字K_0和K_1，这2个关键字在查询阶段没有被查询过，并将它们发送给挑战者$\mathcal{C}$。挑战者$\mathcal{C}$随机选择一个关键字K_x，其中$x\in\{0,1\}$，然后选择一个随机数r，并执行关键词陷门生成算法TrapdoorGen，计算$\text{TD}_1=g_1^{b}H_1(K_x)^{r}$和$\text{TD}_2=g^{r}$。然后挑战者$\mathcal{C}$将检索陷门$\text{TD}_{k_x}=(\text{TD}_1,\text{TD}_2)$发送给敌手$\mathcal{A}$。

猜测。在查询了N个不同的关键字之后，敌手$\mathcal{A}$猜测陷门，并输出x'。如果$x'=x$，则表示敌手$\mathcal{A}$能够区分关键字K_0和K_1，敌手$\mathcal{A}$获胜。

如果敌手$\mathcal{A}$能够在猜测阶段以不可忽略的优势赢得游戏，这意味着挑战者$\mathcal{C}$可以解决PPT中的离散对数问题，这显然是错误的。此外，由于H_1是单向哈希函数，并且在关键字陷门计算中引入了随机数，所以攻击者无法根据$H_1(K_x)^{r}$获取关键字K_x，从而无法正确区分陷门以获取私人信息。因此，在随机预言模型下，任何敌手都不能以不可忽略的优势打破本文方案的KGA安全性。证毕。

5.3 隐私保护分析

本节首先介绍加解密过程的隐私保护，然后介绍智能合约所提供的数据搜索的隐私保护，最后阐述所设计的医疗数据分享协议流程的隐私保护。

1) 加解密过程的隐私保护。在本文方案中，医院使用安全算法对所有医疗数据进行加密并上传。假设加密算法在安全模型中足够安全，那么任何不符合权限或没有解密密钥的实体都无法解密密文。因此，云服务器无法从密文中推断出任何明文医疗数据的相关信息。此外，只有密文数据属性满足MRI的访问结构时，云服务器才会对密文进行部分解密，并且只有当MRI拥有解密密钥DeKey时，才能对转换密文进行解密，获取明文数据。

2) 数据搜索的隐私保护。在本文方案中，医疗数据检索结果由智能合约给出。智能合约的特点保证了检索结果的可信性。MRI会根据其数据需求生成相对应的陷门，智能合约将根据陷门检索相应的数据。云服务器只会接收与关键字匹配的医疗数据密文地址，而且云服务器只能对数据属性满足MRI特定属性需求的密文进行半解密，并将半解密密文传输给MRI以进行最终解密，从而确保了数据搜索的隐私保护。

3) 医疗数据分享协议流程的隐私保护。首先，在分享医疗数据的过程中，医疗数据由KP-ABE加密后上传，其他实体无法获取隐私数据的明文。其次，医院与MRI之间没有直接交互，而是由智能合约完成。由于智能合约只能获取与关键字相关的密文索引，而非原始隐私数据，所以任何与智能合约交互的实体都无法窃取隐私数据。最后，本文方案使用哈希函数和随机数对关键字进行加密，可以保证关键字的安全性，使得用户的隐私信息不会通过关键字泄露。

5.4 功能分析

本节将本文方案与文献[13]、文献[15]、文献[17]和文献[31-33]进行功能方面的比较，结果如表4所示。

表4　功能分析

方案	区块链	细粒度访问	外包解密机制	智能合约搜索
文献[13]	√	×	×	×
文献[15]	√	×	×	×
文献[17]	√	√	√	×
文献[31]	×	√	√	×
文献[32]	×	√	×	×
文献[33]	×	√	×	×
本文方案	√	√	√	√

本文方案和文献[17]、文献[31-33]均能实现细粒度数据访问控制，但本文方案是基于KP-ABE算法的，相较于其他基于CP-ABE算法的方案，KP-ABE更直接地满足数据用户的需求，因为KP-ABE使得用户仅解密满足特定属性需求的数据。本文方案与文献[13]、文献[15]和文献[17]均采用区块链技术，同时本文方案和文献[17]、文献[31]的工作引入了外包解密机制减少解密开销。另外，与其他方案相比，本文方案提供了安全的关键字检索功能，尽管文献[17]和文献[33]也提供了关键字检索功能，但在本文方案中，关键字检索能够由区块链智能合约执行，确保检索结果是完全可信性的。

5.5　性能分析

表5对比了本文方案与其他现有方案在密钥生成、加密、陷门生成、搜索和解密方面的计算复杂度，其中E和E_t分别表示G_1群和G_T群上的一次指数运算，M_1和M_t分别表示G_1群和G_T群上的一次乘法运算，P和H分别表示一次双线性配对和一次哈希计算，U表示系统属性空间大小，f表示访问结构或用户属性集中的属性数量，S表示满足访问结构的最小属性集数量，k表示关键字数量。表5中“—”表示该方案不涉及此项计算。在本文方案中，密钥生成包括访问控制密钥生成和中间密钥生成，其中访问控制密钥生成的计算量为$(2+U)fE$，中间密钥生成的计算量为$(1+U)fE$。从表5可以看出，本文方案的加解密复杂度皆为常量级，并且解密仅涉及G_T群上的一次指数运算。

5.6　实验评估

为了对本文方案进行实验测试和性能分析，本实验在配置为12th Gen Intel(R) Core(TM) i7-12700 2.10 GHz处理器，16 GB RAM和64 bit Windows操作系统的个人计算机上，使用内存为4 GB的本地虚拟机Ubuntu 20.04进行实验仿真。实验基于SpringBoot搭建了医疗系统，其中引入JPBC（java pairing-based cryptography library）库实现加解密算法，并选取A型椭圆曲线$y^2=x^3+x$作为双线性映射曲线。智能合约使用Rust编程语言编写，通过本地Substrate dev区块链辅助构建，并在本地环境安装substrate-contracts-node节点后，利用Substrate contract UI平台进行部署。实验所采用的医疗数据来自于阿里云天池实验室的患者治疗与健康记录数据集，每一条数据都包含以下字段：患者ID、年龄、性别、疾病类型、疾病严重程度、治疗方案、项目检查、遗传病史以及数据关键字等。本文基于此数据集对所提方案进行性能评估。

表6展示了本文方案所涉及的E、E_t、M_1、M_t、P和H这些基础运算的时间消耗，其数据来自多次测试所得的平均值。表7展示了智能合约中单次乘法运算和配对运算的时间消耗，其中Substrate框架下的智能合约是以refTime表示用于执行的计算时间，以皮秒（ps）为单位。

因为文献[17]和文献[33]基于CP-ABE算法，而文献[34]和本文方案基于KP-ABE算法。所以，在文献[17]和文献[33]中，隐私数据由访问结构加

表5　性能分析

方案	密钥生成	加密	陷门生成	搜索	解密
文献[17]	$(5f+9)E$	$(4f+2)E+E_t+P$	$(k+1)E+E_t+P+kH$	$E+kE_t+P$	E_t
文献[31]	$(2f+3)E$	$(5f+2)E+3E_t$	—	—	$2P+2(S+1)$
文献[32]	$(3f+2)E$	$(3f+2)E+E_t$	—	—	$2E+fE_t+3P$
文献[33]	$4fE$	$(2f+4)E+3E_t+(2f+1)P$	$(kf+1)E+P$	$(2f+1)E+3E_t+3P$	$2E_t$
文献[34]	$(7f+4fU+1)E$	$2E+2E_t+H+P$	M_1+H	$2fE+2P+(f^2+f-1)M$	E_t
本文方案	$(3+2U)fE$	$4E+E_t+H$	$3E+H$	$2P+M_t$	E_t

密，而在文献[34]和本文方案中，隐私数据由属性集加密。本文将数据所有者访问结构中的属性数量和数据所有者属性集中的数量统称为DO的属性数量。此外，在文献[17]和文献[33]中，密钥与数据用户的属性集相关联，而在文献[34]和本文方案中，密钥与数据用户的访问结构相关联。因此，本文将数据用户访问结构中的属性数量和数据用户属性集中的数量统称为DU的属性数量。

表6　　基础运算的时间消耗

单次基础运算	时间消耗
E	10.29 ms
E_t	0.78 ms
M_1	81.51 μs
M_t	26.50 μs
H	60.28 μs
P	6.57 ms

表7　智能合约中单次乘法运算和配对运算的时间消耗

单次基础运算	时间消耗/ps
M_t	798 333 337
P	83 963 826 183

首先，本文评估了系统属性域大小对访问控制密钥$\mathrm{ACSK}_{(\boldsymbol{M},\rho)}$和中间密钥InterKey生成的影响。实验将系统属性域大小分别设置为20、30和40，然后依次测试访问结构中属性数量为5~20时访问控制密钥$\mathrm{ACSK}_{(\boldsymbol{M},\rho)}$和中间密钥InterKey的生成时间。实验结果如图6和图7所示。

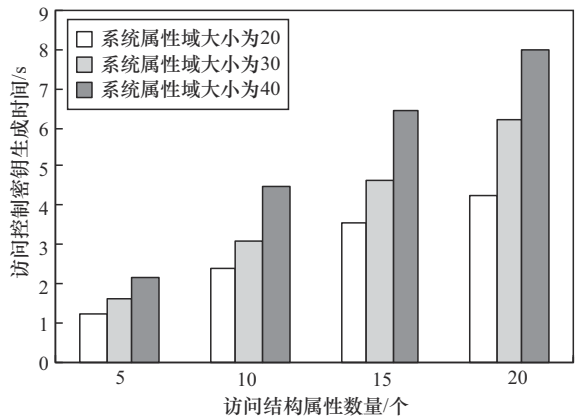


图6　访问控制密钥生成时间

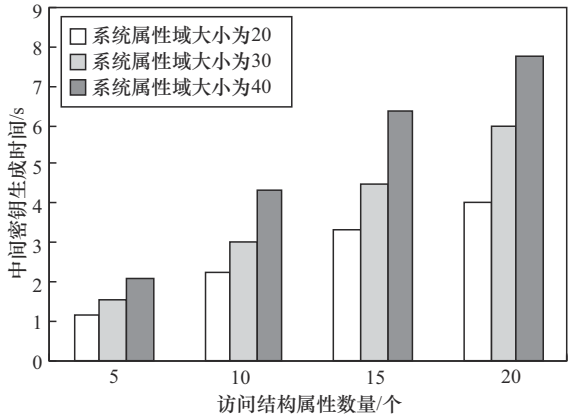


图7　中间密钥生成时间

从图6和图7中可以看到，当访问结构中属性数量保持不变时，访问控制密钥$\mathrm{ACSK}_{(\boldsymbol{M},\rho)}$和中间密钥InterKey的生成时间与系统属性域大小呈线性增长。当系统属性域大小不变时，访问控制密钥$\mathrm{ACSK}_{(\boldsymbol{M},\rho)}$和中间密钥InterKey的生成时间随着访问结构中属性数量的增加而增加。实验结果与表5中的理论分析一致。

图8分析了该方案中所有密钥生成时间的总和，包括访问控制密钥$\mathrm{ACSK}_{(\boldsymbol{M},\rho)}$和中间密钥InterKey的生成时间总和。由于密钥生成时间与系统属性域大小相关，当DU的属性数量相同时，本文方案中所有密钥生成的成本高于文献[17]和文献[33]中的成本，但优于文献[34]，生成时间几乎是文献[34]的一半。

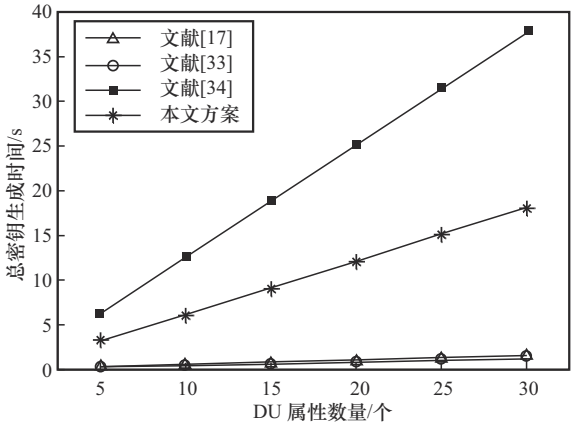


图8　总密钥生成时间

本文方案采用了属性基加密算法，为了探究属性数量对加密性能的影响，本文在一个系统属性域大小设置为30的系统环境下进行了实验。在实验

中，逐步将DO的属性数量从5递增至30进行测试。本文方案与文献[17]、文献[33]和文献[34]比较的实验结果如图9所示，显然本文方案的加密时间与文献[34]相似，明显优于文献[17]和文献[33]。具体来说，本文方案中的加密算法几乎不受DO属性数量的影响，加密时间恒定为40 ms，而文献[17]和文献[33]中的加密时间随着DO属性数量的增加而增加。当DO的属性数量为30时，文献[17]和文献[33]的加密时间超过1 s。

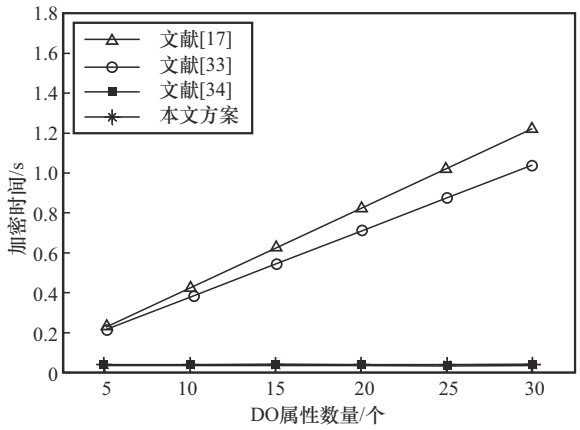


图9　加密时间

由于文献[17]和文献[33]可以进行多关键字搜索，实验中比较陷门生成时间时，设置关键字数量 $k = 1$。如图10所示，本文方案的陷门生成性能处于中等水平。

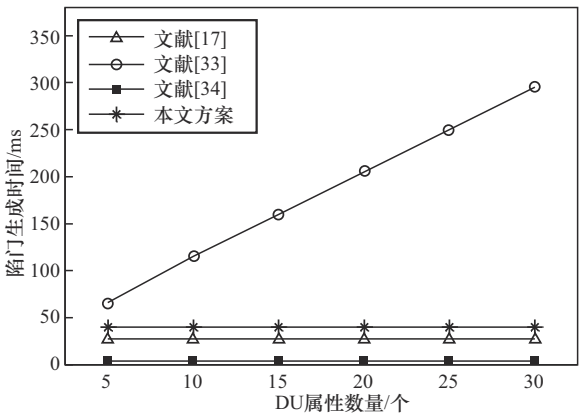


图10　陷门生成时间

如图11所示，本文方案将搜索算法与文献[33]和文献[34]进行了比较。本文方案中的搜索仅需要进行两次配对运算和一次 G_T 群上的乘法运算，与DU的属性数量无关。本文方案的单次搜索时间稳定在12 ms左右，远优于文献[33]和文献[34]。

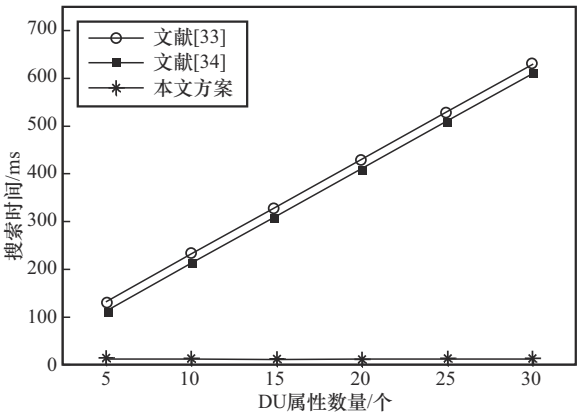


图11　搜索时间

引入智能合约后，搜索时间会有所增加。通过100次搜索测试，发现不使用智能合约的单次平均搜索时间为12 ms，而使用智能合约的单次平均搜索时间为200 ms。智能合约中执行双线性计算的复杂性，是造成搜索时间增长的主要原因。然而，通过智能合约进行检索可以有效抵御恶意云服务器攻击，使其成为在搜索安全性需求高于搜索速度需求的场景下的可行选择。

图12展示了DU属性数量对解密性能的影响。在本文方案中，大量的解密操作外包给云服务器。因此，用户只需要根据云服务器的解密结果执行指数运算操作。

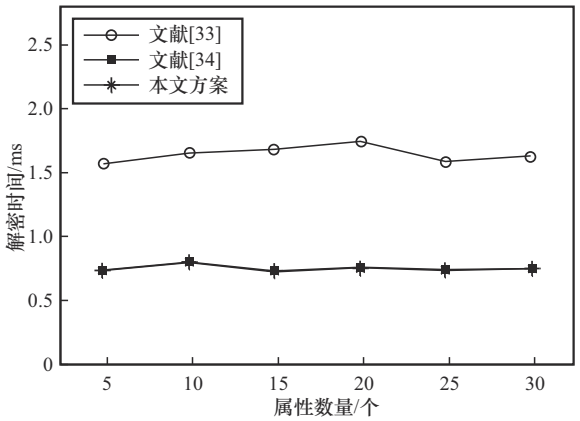


图12　解密时间

最后，实验测试了本文方案的各部分在系统中的总时间开销，如表8所示，其中系统属性空间大小设为30，用户的数据需求访问结构包括5个属性，本地数据库由阿里云天池实验室的患者治疗与健康记录数据集中的1 000份医疗记录组成，其中

10%的数据满足搜索需求。

表 8 系统总时间开销

步骤	时间开销
数据加密	39.375 s
数据解密	87.012 ms
用户密钥生成	3.256 s
智能合约下的数据搜索	168 893 913 355 366 ps

总之，在用户密钥生成、陷门生成操作中，本文方案性能适中。在数据加密、解密和搜索操作中，本文方案性能最优。此外，本文方案搜索操作可以由区块链智能合约执行。因此，本文方案可以提供高效且安全的搜索操作。

6 结束语

本文提出了一种基于区块链的轻量级且安全的数据搜索方案。为了在数据安全性和可用性之间取得平衡，本文设计了一套轻量级的搜索算法，仅涉及一次乘法运算和两次配对运算，因而通过引入智能合约来代替云服务器执行搜索具有可行性，而且克服了不可信第三方所引起的搜索安全问题。另外，本文方案将所设计的轻量级搜索算法与可外包的KP-ABE结合，实现了对搜索结果的细粒度访问控制。最后，通过安全性分析和性能实验证明了本文方案的安全性和可行性。

然而，本文方案仍存在一些不足，主要包括两方面。1) 虽然本文设计了较轻量级的搜索算法，使得引入智能合约执行安全搜索变得可行，但是因为其存在配对运算，所需的消耗未减小到理想值。下一步希望设计出更加轻量级的搜索算法，以达到降低消耗改善和改善搜索效率的目的。2) 随着医疗数据的不断增多，搜索时间随之变长，数据存储空间也随之变大，未来考虑在保证安全性的前提下进一步优化方案性能以及存储开销。

附录 1 式(30)的详细计算过程

MRI通过最终解密计算$\mathrm{CT}_1\mathrm{TranCT}^{\frac{1}{d}}$恢复医疗数据明文，解密计算的正确性证明过程如式(38)所示。

$$
\begin{aligned}
\mathrm{CT}_1\mathrm{TranCT}^{\frac{1}{d}} &= \left(\frac{e\left(\mathrm{CT}_3,\prod_{k\in\Omega}\left(A_{2,k}'\right)^{v_k}\right)}{e\left(\mathrm{CT}_2,\prod_{k\in\Omega}\left(A_{1,k}'\prod_{\Upsilon}A_{3,k,i}'\right)^{v_k}\right)}\right)^{\frac{1}{d}}\mathrm{CT}_1 = \left(\frac{e\left((T_0\prod_{\mathrm{att}_i\in\mathrm{attSet}}t_{\mathrm{att}_i})^{s},\prod_{k\in\Omega}\left(g^{dc_k}\right)^{v_k}\right)}{e\left(g^{s},\prod_{k\in\Omega}\left(g^{d\lambda_{\rho(k)}}(T_0t_{\rho(k)})^{dc_k}\prod_{\Upsilon}t_{\mathrm{att}_i}^{dc_k}\right)^{v_k}\right)}\right)^{\frac{1}{d}}\mathrm{CT}_1 = \\
&\left(\frac{e\left((T_0\prod_{\mathrm{att}_i\in\mathrm{attSet}}t_{\mathrm{att}_i})^{s},\prod_{k\in\Omega}\left(g^{dc_k}\right)^{v_k}\right)}{e\left(g^{s},\prod_{k\in\Omega}g^{dv_k\lambda_{\rho(k)}}\prod_{k\in\Omega}\left(T_0t_{\rho(k)}\prod_{\Upsilon}t_{\mathrm{att}_i}\right)^{dc_kv_k}\right)}\right)^{\frac{1}{d}}\mathrm{CT}_1 = \left(\frac{e\left((T_0\prod_{\mathrm{att}_i\in\mathrm{attSet}}t_{\mathrm{att}_i})^{s},g^{d\sum_{k\in\Omega}c_kv_k}\right)}{e\left(g^{s},g^{d\sum_{k\in\Omega}v_k\lambda_{\rho(k)}}\left(T_0\prod_{\mathrm{att}_i\in\mathrm{attSet}}t_{\mathrm{att}_i}\right)^{d\sum_{k\in\Omega}c_kv_k}\right)}\right)^{\frac{1}{d}}\mathrm{CT}_1 = \\
&\left(\frac{e\left((T_0\prod_{\mathrm{att}_i\in\mathrm{attSet}}t_{\mathrm{att}_i})^{d\sum_{k\in\Omega}c_kv_k},g^{s}\right)}{e\left(g^{s},g^{da}\right)e\left((T_0\prod_{\mathrm{att}_i\in\mathrm{attSet}}t_{\mathrm{att}_i})^{d\sum_{k\in\Omega}c_kv_k},g^{s}\right)}\right)^{\frac{1}{d}}\mathrm{CT}_1 = \left(\frac{1}{e\left(g^{s},g^{da}\right)}\right)^{\frac{1}{d}}\mathrm{msg}Y^{s} = \left(\frac{1}{e\left(g^{s},g^{da}\right)}\right)^{\frac{1}{d}}\mathrm{msg}e(g,g)^{as} = \mathrm{msg}
\end{aligned}
\tag{38}
$$

其中，Ω表示所有满足$\rho_{(k)}\in\mathrm{attSet}$的$k$的集合，$\Upsilon=\left\{\mathrm{att}_i\in\mathrm{attSet}\backslash\rho_{(k)}\right\}$表示属性$\mathrm{att}_i$在医院的属性集合attSet中，但不包括$\rho_{(k)}$对应的属性。

附录 2 式(31)正确性证明

智能合约可以通过验证等式$e\left(\mathrm{TD}_2,I_3\right)I_1=e\left(\mathrm{TD}_1,I_2\right)$是否成立来检验数据是否匹配，其计算的正确性证明过程如

式(39)和式(40)所示。

$$e\left(\mathrm{TD}_2,I_3\right)I_1=e\left(g^{r_1},H\left(\mathrm{kwd}\right)^r\right)e\left(g_1,g^b\right)^r=$$
$$e\left(g,H\left(\mathrm{kwd}\right)^{rr_1}\right)e\left(g_1,g^b\right)^r \tag{39}$$

$$e\left(\mathrm{TD}_1,I_2\right)=e\left(g_1^bH\left(\mathrm{Sekeyword}\right)^{r_1},g^r\right)=$$
$$e\left(g_1^b,g^r\right)e\left(H\left(\mathrm{Sekeyword}\right)^{r_1},g^r\right)=$$
$$e\left(g_1,g^b\right)^re\left(H\left(\mathrm{Sekeyword}\right),g\right)^{rr_1} \tag{40}$$

若kwd = Sekeyword，则式(39)与式(40)的结果相等，则表明等式$e\left(\mathrm{TD}_2,I_3\right)I_1=e\left(\mathrm{TD}_1,I_2\right)$成立。

参考文献：

[1] 张晓旭, 陈宇辰, 哈冠雄, 等. 基于分布式存储的外包EHR隐私保护分类审计方案[J]. 通信学报, 2024, 45(9): 26-39.
ZHANG X X, CHEN Y C, HA G X, et al. Classification auditting scheme for privacy protection of outsourced EHR based on distributed storage[J]. Journal on Communications, 2024, 45(9): 26-39.

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

[3] GE C P, SUSILO W, LIU Z, et al. Secure keyword search and data sharing mechanism for cloud computing[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(6): 2787-2800.

[4] MIAO Y B, DENG R H, CHOO K K R, et al. Threshold multi-keyword search for cloud-based group data sharing[J]. IEEE Transactions on Cloud Computing, 2022, 10(3): 2146-2162.

[5] YANG Y, ZHANG Y C, LIU J, et al. Chinese multi-keyword fuzzy rank search over encrypted cloud data based on locality-sensitive hashing[J]. Journal of Information Science and Engineering, 2019, 35(1): 137-158.

[6] YIN H, QIN Z, ZHANG J X, et al. A fine-grained authorized keyword secure search scheme with efficient search permission update in cloud computing[J]. Journal of Parallel and Distributed Computing, 2020, 135: 56-69.

[7] WANG H J, DONG X L, CAO Z F. Multi-value-independent ciphertext-policy attribute based encryption with fast keyword search[J]. IEEE Transactions on Services Computing, 2020, 13(6): 1142-1151.

[8] MIAO Y B, MA J F, LIU X M, et al. Attribute-based keyword search over hierarchical data in cloud computing[J]. IEEE Transactions on Services Computing, 2020, 13(6): 985-998.

[9] 牛淑芬, 谢亚亚, 杨平平, 等. 区块链上基于云辅助的属性基可搜索加密方案[J]. 计算机研究与发展, 2021, 58(4): 811-821.
NIU S F, XIE Y Y, YANG P P, et al. Cloud-assisted attribute-based searchable encryption scheme on blockchain[J]. Journal of Computer Research and Development, 2021, 58(4): 811-821.

[10] YU J G, LIU S H, XU M H, et al. An efficient revocable and searchable MA-ABE scheme with blockchain assistance for C-IoT[J]. IEEE Internet of Things Journal, 2023, 10(3): 2754-2766.

[11] TANG X Y, GUO C, CHOO K K R, et al. A secure and trustworthy medical record sharing scheme based on searchable encryption and blockchain[J]. Computer Networks, 2021, 200: 108540.

[12] 杜瑞忠, 谭艾伦, 田俊峰. 基于区块链的公钥可搜索加密方案[J]. 通信学报, 2020, 41(4): 114-122.
DU R Z, TAN A L, TIAN J F. Public key searchable encryption scheme based on blockchain[J]. Journal on Communications, 2020, 41 (4): 114-122.

[13] LAI C Z, MA Z, GUO R, et al. Secure medical data sharing scheme based on traceable ring signature and blockchain[J]. Peer-to-Peer Networking and Applications, 2022, 15(3): 1562-1576.

[14] HUANG H P, ZHU P, XIAO F, et al. A blockchain-based scheme for privacy-preserving and secure sharing of medical data[J]. Computers and Security, 2020, 99: 102010.

[15] KAUR J, RANI R, KALRA N. A blockchain-based framework for privacy preservation of electronic health records (EHRs)[J]. Transactions on Emerging Telecommunications Technologies, 2022, 33(9): e4507.

[16] LIU J W, WU M L, SUN R, et al. BMDS: a blockchain-based medical data sharing scheme with attribute-based searchable encryption[C]// Proceedings of the ICC 2021-IEEE International Conference on Communications. Piscataway: IEEE Press, 2021: 1-6.

[17] XU G Q, QI C, DONG W Y, et al. A privacy-preserving medical data sharing scheme based on blockchain[J]. IEEE Journal of Biomedical and Health Informatics, 2023, 27(2): 698-709.

[18] BONEH D, CRESCENZO G D, OSTROVSKY R, et al. Public key encryption with keyword search[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2004: 506-522.

[19] ZHENG Q J, XU S H, ATENIESE G. VABKS: verifiable attribute-based keyword search over outsourced encrypted data[C]//Proceedings of the IEEE INFOCOM 2014-IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2014: 522-530.

[20] CHAUDHARI P, DAS M L. KeySea: keyword-based search with receiver anonymity in attribute-based searchable encryption[J]. IEEE Transactions on Services Computing, 2022, 15(2): 1036-1044.

[21] GU K, ZHANG W B, LI X, et al. Self-verifiable attribute-based keyword search scheme for distributed data storage in fog computing with fast decryption[J]. IEEE Transactions on Network and Service Management, 2022, 19(1): 271-288.

[22] SANGEETHA D, CHAKKARAVARTHY S S, SATAPATHY S C, et al. Multi keyword searchable attribute based encryption for efficient retrieval of health records in cloud[J]. Multimedia Tools and Applications, 2022, 81(16): 22065-22085.

[23] XIANG X Y, ZHAO X W. Blockchain-assisted searchable attribute-based encryption for e-health systems[J]. Journal of Systems Architecture, 2022, 124: 102417.

[24] ZHAO F, PENG C G, XU D Q, et al. Attribute-based multi-user collaborative searchable encryption in COVID-19[J]. Computer Communications, 2023, 205: 118-126.

[25] GAO H C, HUANG H P, XUE L Y, et al. Blockchain-enabled fine-grained searchable encryption with cloud-edge computing for electronic health records sharing[J]. IEEE Internet of Things Journal, 2023, 10(20): 18414-18425.

[26] CHEN B W, XIANG T, HE D B, et al. BPVSE: publicly verifiable searchable encryption for cloud-assisted electronic health records[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 3171-3184.

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

[28] LEWKO A, WATERS B. Decentralizing attribute-based encryption[C]// Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2011: 568-588.

[29] 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.

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

[31] ZENG P, ZHANG Z T, LU R X, et al. Efficient policy-hiding and large universe attribute-based encryption with public traceability for Internet of medical things[J]. IEEE Internet of Things Journal, 2021, 8(13): 10963-10972.

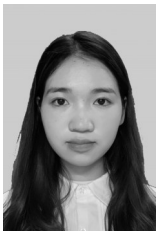
[32] 李琦, 朱洪波, 熊金波, 等. mHealth中可追踪多授权机构基于属性的访问控制方案[J]. 通信学报, 2018, 39(6): 1-10.
LI Q, ZHU H B, XIONG J B, et al. Multi-authority attribute-based access control system in mHealth with traceability[J]. Journal on Communications, 2018, 39(6): 1-10.

[33] ZHANG K, LONG J H, WANG X F, et al. Lightweight searchable encryption protocol for industrial Internet of things[J]. IEEE Transactions on Industrial Informatics, 2021, 17(6): 4248-4259.

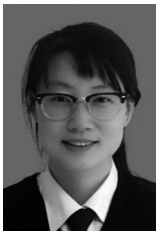
[34] BAO Y Y, QIU W D, CHENG X C. Secure and lightweight fine-grained searchable data sharing for IoT-oriented and cloud-assisted smart healthcare system[J]. IEEE Internet of Things Journal, 2022, 9(4): 2513-2526.

［作者简介］

谢晴晴（1990– ），女，安徽宿州人，博士，江苏大学讲师，主要研究方向为区块链、应用密码学。



宋亮晴（2000– ），女，湖南长沙人，江苏大学硕士生，主要研究方向为区块链、应用密码学等。



冯霞（1983– ），女，江苏镇江人，博士，海南大学教授，主要研究方向为物联网安全、区块链、应用密码学。