王燕, 巫朝霞. 云医疗中基于非对称配对的属性基可搜索加密方案[J]. 智能计算机与应用,2025,15(9):41-48. DOI:10.20169/j.issn.2095-2163.25052703

云医疗中基于非对称配对的属性基可搜索加密方案

王 燕, 巫朝霞
(新疆财经大学 统计与数据科学学院, 乌鲁木齐 830012)

摘 要: 随着云医疗技术的快速发展,传统的纸质医疗档案正在逐步被电子健康档案替代,因此云医疗数据安全且有效共享成为了一个亟待解决的关键问题。为解决这一问题,提出了一个在云医疗中基于非对称配对的属性基可搜索加密方案。该方案利用访问树构造访问策略,用非对称配对设置基于属性的可搜索加密,将数据加密、关键字搜索与访问策略相结合来实现数据的细粒度搜索;通过引入版本密钥到属性密钥中,结合版本密钥的更新机制,实现密钥和密文的同步更新,从而支持属性的及时撤销;将涉及关键字和属性的加解密计算任务外包给云服务器,降低本地设备的计算负担。安全性分析、性能分析和实验分析表明,该方案具有安全性强、计算量低和运行时间短的特点,能在保护患者隐私的情况下有效实现云医疗数据的安全共享。

关键词: 电子健康档案; 非对称配对; 细粒度搜索; 属性撤销; 外包加解密
中图分类号: TP309 **文献标志码**: A **文章编号**: 2095-2163(2025)09-0041-08

Asymmetric pairing-based attribute-based encryption scheme in cloud healthcare

WANG Yan, WU Zhaoxia
(School of Statistics and Data Science, Xinjiang University of Finance and Economics, Urumqi 830012, China)

Abstract: With the rapid development of cloud medical technology, traditional paper medical records are gradually being replaced by Electronic Health Records. Therefore, the secure and effective sharing of cloud medical data has become a key issue that urgently needs to be solved. To solve this problem, an attribute-based searchable encryption scheme based on asymmetric pairing in cloud healthcare is proposed. This scheme uses the access tree to construct the access policy, sets the attribute-based searchable encryption with asymmetric pairing, and combines data encryption, keyword search and access policy to achieve fine-grained data search. By introducing the version key into the attribute key and combining with the update mechanism of the version key, the synchronous update of the key and ciphertext is achieved, thereby supporting the timely revocation of attributes. The encryption and decryption computing tasks involving keywords and attributes are outsourced to the cloud server to reduce the computing burden of local devices. Security analysis, performance analysis and experimental analysis show that this scheme has the characteristics of strong security, low computational complexity and short running time, and can effectively achieve the secure sharing of cloud medical data while protecting patients' privacy.

Key words: Electronic Health Record; asymmetric pairing; fine-grained search; attribute revocation; outsourced encryption and decryption

0 引 言

随着云计算技术的发展与应用,传统纸质医疗记录正逐渐被电子健康档案(Electronic Health Record,EHR)所替代[1]。相较于传统的纸质记录,EHR 有着节省存储空间、提高工作效率、医疗信息可以实时更新等诸多显著的优势。因此 EHR 数据安全且有效共享成为了亟待解决的关键问题。

CP-ABE 方案首先由 Sahai 等学者[2]提出,其核心在于只有当数据使用者的属性集合与加密文本中设定的访问条件相匹配时,该使用者方能成功解密信息。这一机制有效保障了仅有获得授权的个体(例如病患、医护人员)能够访问病患的电子健康记录,从而强化数据隐私防护措施。

基金项目: 新疆维吾尔自治区自然科学基金面上项目(2024D01A37)。
作者简介: 王 燕(2001—),女,硕士研究生,主要研究方向:云数据安全。
通信作者: 巫朝霞(1978—),女,博士,硕士生导师,主要研究方向:信息安全研究。Email:wuzhaoxia828@163.com。
收稿日期: 2025-05-27

然而,CP-ABE 方案仍然面临着许多挑战,例如:为了便于用户查询,需要支持细粒度搜索;由于用户属性可能动态变化,需实时处理属性撤销问题。文献[3]建议为每个用户属性设置有效期,并由属性授权机构定期发布密钥更新参数。文献[4]提出基于二叉树结构实现用户的属性撤销。文献[5]提出在被撤销用户中加入标识"非",使之不能解密对应数据。文献[6]提出一种混合撤销的 CP-ABE 方案,支持数据拥有者选择直接和间接撤销的方式。

CP-ABE 方案因繁复的数学运算对设备施加了沉重的计算负荷,文献[7]提出了将解密任务外包的策略,以减轻用户端的计算压力。文献[8]提出了将加密与解密双重外包的策略。文献[9]的方案是将与属性相关的加解密计算都外包。

但以上方案在属性撤销方面进行改进的方案存在效率不高、不能更改或不能实现立即撤销的问题;而减轻负担方面又存在未有效缓解数据所有者在加密阶段所面临的工作量问题。因此,一个既能实现数据的细粒化共享,又能对数据的共享权限实时进行调整,还能减少本地计算开销的加密方案就显得尤为重要。

针对该问题,本文提出了一个云医疗中基于非对称配对的属性基可搜索加密方案,采用访问树构建访问策略,非对称配对技术设置基于属性的可搜索加密,将数据加密、关键字检索与访问控制策略紧密结合实现数据的细粒度搜索;将版本密钥加入属性密钥之中,借助其动态更新机制,实现密钥与密文的同步更新,从而支持属性的实时撤销功能;将涉及关键字和属性的加密与解密操作委托给云服务器执行,降低所有者在本地设备的计算负担。

1 基础知识

文中方案将双线性映射的非对称配对用于加解密,访问树结构用于访问策略的构造,困难假设讨论 DBDH 假设和 DDH 假设。

1.1 双线性映射

假设 G_1、G_2 和 G_K 是素数阶为 q 乘法循环群,g_1、g_2 分别是 G_1、G_2 的生成元,e 是双线性映射,$e:G_1 \times G_2 \rightarrow G_K$。如果 $G_1 = G_2$,则称配对是对称的(Type-Ⅰ配对);如果 $G_1 \neq G_2$,则称配对是非对称的,如果 G_1 和 G_2 之间没有已知的有效同构性,则称该配对为 Type-Ⅲ配对[10]。双线性映射 e 具有下面 3 个性质:

(1)双线性:对于任意 $g_1 \in G_1, g_2 \in G_2, \{c,d\} \in Z_q^*$,使得等式 $e(g_1{}^c, g_2{}^d) = e(g_1, g_2)^{cd}$ 均成立。

(2)非简并性:存在 $g_1 \in G_1, g_2 \in G_2$,使得 $e(g_1, g_2) \neq 1$ 成立。

(3)可计算性:对任意 $g_1 \in G_1, g_2 \in G_2$,有一个多项式算法可以有效地计算 $e(g_1, g_2)$。

1.2 访问树结构

树形访问结构 TR 中,所有非叶子节点都是带有阈值的门限方案。对于节点 j,假设子节点的数量为 num_j,节点的门限值为 k_j。当 $k_j = 1$ 时,节点 j 的门限门是"或"门;当 $k_j = \text{num}_j$ 时,节点 j 的门限门是"与"门。设节点 j 的属性为 attr_j,父节点为 $\text{parent}(j)$。设 TR_j 表示以 j 为根节点的 TR 的子树,将 j 的节点从 1 到 num_j 进行排序,$\text{index}(j)$ 表示节点 j 的序号。如果属性集合 F 满足子树 TR_j,记为 $\text{TR}_j(F) = 1$。

1.3 困难假设

DBDH(Decisional Bilinear Diffie-Hellman)假设[9]:G 表示阶数为素数 q 的乘法循环群,生成元为 g,随机选择 $m,n,r,t \in Z_q$,给定 $(g, g^m, g^n, g^r, e(g,g)^{mnr})$ 和 $(g, g^m, g^n, g^r, e(g,g)^t)$ 两个元组,若 DBDH 假设成立,则攻击者无法通过多项式时间算法区分 $e(g,g)^{mnr}$ 和 $e(g,g)^t$。

DDH(Decisional Diffie-Hellman)假设[9]:G 表示阶数为素数 q 的乘法循环群,生成元为 g,随机选择 $m,n,r \in Z_q$,给定 2 个元组 (g^m, g^n, g^r) 和 (g^m, g^n, g^{mn}),若 DDH 假设成立,则攻击者无法通过多项式时间算法区分 g^r 和 g^{mn}。

2 系统模型与安全模型

2.1 系统模型

本文方案由 5 个实体组成,分别是用户、中央授权机构、属性授权机构、数据所有者和云服务器,具体的系统模型如图 1 所示。

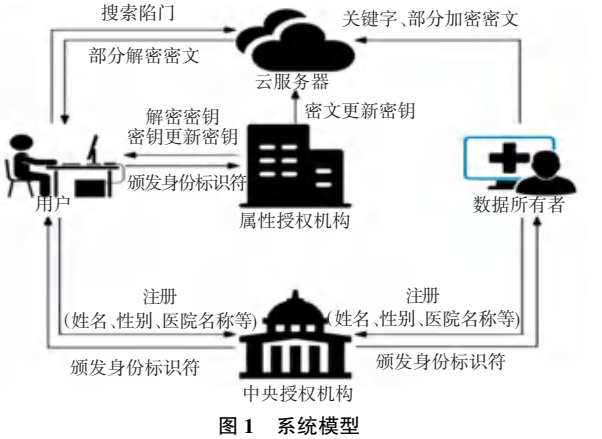

图 1 系统模型

Fig. 1 Model of the system

(1)用户：是指需要访问 EHR 数据的人，包括患者本人、家属或其他被授权解密密文的人。

(2)中央授权机构：负责公共参数的初始配置以及为新用户派发全局身份标识。

(3)属性授权机构：负责分发解密密钥，以及在属性撤销时，计算密钥和密文的更新密钥并发送给云服务器和用户。

(4)数据所有者：需要对部分数据进行加密，并将访问策略、部分密文以及关键词上传至云服务器。

(5)云服务器：主要是用于存储密文数据。不仅需要验证用户属性集是否符合访问策略，还需要在发生属性撤销时，利用更新后的密文对原始加密数据进行重新加密。

2.2　算法形式化定义

本文所提的方案主要包括系统初始化、生成用户密钥、用户加密、云服务器外包加密、生成搜索陷门、云服务去搜索解密、用户解密和属性撤销，其中属性撤销包括属性密钥更新、搜索密钥更新和密文更新。

(1)系统初始化。setup(ψ) → (qq,zmy)：由中央授权机构执行。运算过程中输入安全参数 ψ，输出公共参数 qq = $\{G_1, G_2, e, g_1, g_2, e(g_1,g_2)^v, g_1{}^u, \{qk_x\}_{x\in F}\}$ 和主密钥 zmy = $\{u, v, g_2{}^v, \{uk_x\}_{x\in S}\}$。

(2)生成用户密钥。keygen(qq,zmy,F) → (sy)：由中央授权机构执行。根据 qq、zmy 和系统的属性集 F，生成用户的私钥 sy = $\{k_u, K_x\}$。

(3)用户加密。Encrypt1(f,N) →IT_0：由数据所有者执行。输入系统参数 f 和数据 N，生成部分加密密文 IT_0 =$\{O_0, O_1, (N,\rho)\}$。

(4)云服务器外包加密。Encrypt2(f, (N,ρ), IT_0,qk,V) → (O_2, O_3, IT_x, I_v)：由云服务器完成。运算过程是输入 f、N、IT_0、公钥 qk 和关键字集 V，得到 I_v，输出最终密文 IT = $\{O_0, O_1, O_2, O_3, IT_x I_v\}$ 并存储在与服务器中。

(5)生成搜索陷门。Tapdoor(k_u, K_x,g) → td：由用户执行。运算过程是输入用户密钥 k_u、用户属性密钥 K_x 和关键字 g，生成陷门 td = $\{T_{x,1}, T_{x,2}, T_v\}$。

(6)云服务器搜索解密。Search&Decrypt(I_v, td,IT_x) → (A_t)：由云服务器执行。具体的运算过程是输入关键字索引 I_v、td 和属性密文 IT_x，只有当用户的属性密钥与访问策略成功匹配，才能输出部分解密密文 $A_t = e(g_1,g_2)^{udr^2\zeta}$。

(7)用户解密。Decrypt(k_u, E_t, IT_0, O_3) → (N)：由用户执行。运算过程是输入 k_u、A_t、IT_0 以及 O_3，最终输出明文 N，得到 EHR 数据。

(8)属性撤销

① 属性密钥更新。update_1(x', K_x, $vk_{x'}$) → (sy_u')：由用户执行。输入需要撤销的属性 x'、K_x、和$vk_{x'}$，得到更新后的属性密钥 sy_u'。

② 搜索密钥更新。update_2(sy_u') → (td′)：该算法由用户执行。输入 sy_u'，输出更新后的搜索密钥 td′。

③ 密文更新。update_3($vk_{t'}$,IT_x) → (IT_x')：该算法由云服务器执行。输入 $vk_{t'}$ 和 IT_x，输出更新后的密文 IT_x'。

2.3　安全模型

基于关键字和陷门的不可区分性，使用对手 D 和挑战者 C 之间的安全博弈来定义安全模型[11]。

(1)关键字不可区分

① 初始化：T 通过初始化算法获得 2 个公共参数 qq 和 zmy，将 qq 发送给 D，保存 zmy。

② 阶段 1：T 首先创建 1 个空列表 K 和 2 个空集合 I 与 R。在该阶段 D 可以向 T 查询属性集 F 的密钥。

③ 密钥查询：D 通过 T 对用户 id 的属性集 F 查询得到其私钥 sy_d，再将属性集发送给 T 得到密钥 mk。

④ 挑战：D 向 T 提交 2 个长度相等的消息 n_0 和 n_1，以及 A_0、A_1 和 F_0、F_1。(列表 L 中不存在满足 A_0 和 A_1 的属性集，或不存在满足 U_0 和 U_1 的用户标识)。T 随机选择 $b \in \{0,1\}$，在访问结构 TR_b 和用户标识集 F_b 下对消息 m_b 进行加密，并将生成的密文返回给 D。

⑤ 猜测：D 输出猜测 τ，若 D 获胜，则此时 $\tau = b$。D 在游戏中的优势可定义为：

$$Adv_A^{gjz} = |\ Pr[\tau = b] - 1/2\ | \tag{1}$$

(2)陷门不可区分

①、②、③与关键字不可区分相同。

④ 陷门查询：D 向 T 查询关键字 g，然后 T 通过算法得到搜索陷门 td，并将其返回给 D。

⑤ 挑战：D 将 2 个长度相等的关键字 (g_0、g_1) 提交给 T，T 任意选择 $b \in \{0,1\}$，在访问结构 TR_b 和用户标识集 S_b 下对 g_b 进行加密，生成陷门 td_b，并将其返回给 D。在此阶段，D 可以对任意查询关键字 $g(g \neq g_0, g \neq g_1)$。

⑥ 猜测：与前文类似，但 D 在游戏中的优势定义为：

$$Adv_A^{xm} = |\ Pr[\tau = b] - 1/2\ | \tag{2}$$

3 属性基可搜索加密的改进方案

在本研究中,设计了一种适用于云医疗的基于非对称配对的属性基可搜索加密方案。该方案在可搜索机制[11]和撤销机制[12]基础上进行了优化,支持细粒度搜索、属性撤销以及加解密任务的外包处理,从而提升了系统的灵活性和实用性。主要包括以下 4 个阶段。

3.1 系统设置

在系统设置阶段,主要是实现系统初始化和生成用户密钥。

(1)系统初始化。setup(ψ) → (qq,zmy)。该算法输入系统安全参数 ψ,G_1、G_2 和 G_K 是素数阶为 q 乘法循环群,g_1、g_2 分别是 G_1 和 G_2 的生成元,定义双线性映射 $e:G_1 \times G_2 \to G_K$,哈希函数 $H_1:\{0,1\}^* \to G_2$,$H_2:\{0,1\}^* \to Z_q^*$,中央授权机构在用户注册时为其分配全局身份标识符 uud。

属性授权机构选取 qq、zmy 和随机数 $u,v \in Z_q^*$,其中 qq 由属性机构公开,zmy 由属性机构秘密保存。属性机构会为每一个属性选择一个版本密钥 $uk_x \in Z_q^*$,首先计算公钥的具体值,公钥 $qk_x = H_1(x)^{uk_x}$,在最后输出公共参数为:$qq = \{G_1, G_2, e, g_1, g_2, e(g_1,g_2)^v, g_1^u, \{qk_x\}_{x\in F}\}$,主密钥为:$zmy = \{u, v, g_2^v, \{uk_x\}_{x\in S}\}$。

(2)生成用户密钥。keygen(qq,zmy,F) → (sy)。使用密钥生成算法输入 qq、zmy 和属性集 F,最后输出私钥 sy,根据 uud 分配对应的属性集 F_u。随机生成 $r \in Z_q^*$,对于任意 $x \in F_u$,生成用户密钥 $k_0 = g_2^{r^2}$,$k_1 = g_2^{ur^2}$,$k_2 = g_2^{v+ur^2}$,$k_u = \{k_0, k_1, k_2\}$。对于版本密钥 uk_x,随机选择一个 $t \in Z_q^*$,针对 F 的每个属性,计算 $K_{x,1} = g_1^{-ut}$,$K_{x,2} = g_2^{r^2} \cdot H_1(x)^{uk_x \cdot t}$,生成用户的属性密钥 $K_x = \{K_{x,1}, K_{x,2}\}$。最后,输出用户的私钥 $sy_u = \{k_u, K_x\}$,通过安全传输通道发送给用户。

3.2 加密阶段

加密部分由用户加密、云服务器外包加密和生成搜索陷门三个阶段组成。

(1)用户加密。Encrypt1(f,N) →IT_0。根据用户属性访问树叶子节点匹配,创建内部节点设置门限阈值、创建叶子节点绑定属性名称和公钥参数,构建访问树 TR,用户选取一个 $f \in Z_q^*$ 的随机数,计算 $O_0 = N \cdot e(g_1,g_2)^{vf}$,$O_1 = g_1^f$,用户提取 HER 文件的关键字集合为 $V = \{v_1, v_2, \cdots, v_n\}$,将部分密文 $IT_0 = \{O_0, O_1, TR\}$ 和关键字集合 V 上传到云服务器。

(2)云服务器外包加密。Encrypt2(f, (N,ρ), IT_0,qk,V) → (O_2,O_3,IT_x,I_v)。云服务器根据用户上传的访问树结构 TR,随机选择一个向量 $w = (d, w_2, \cdots, w_n)$,其中 $w_2, \cdots, w_n \in Z_q^*$,并随机选取秘密值 $d \in Z_q^*$。定义向量 $\eta_x = N_x \cdot w (1 \leqslant x \leqslant n)$,计算 $O_2 = g_1^d$,$O_3 = O_1 \cdot g_1^d = g_1^{f+d}$;对于每个属性 X,计算属性密文 $O_{4,x} = (qk_x)^{\eta_x} = H_1(x)^{uk_x \cdot \eta_x}$,$O_{5,x} = g_1^{u \cdot \eta_x}$,生成属性密文集合 $IT = \{O_{4,x}, O_{5,x}\}$;使用秘密值 d 对关键字 v 进行加密,计算得到关键字的密文 $O_v = e(g_1^u, H_1(v)^d)$,$O_v' = g_1^{ud}$,生成关键字索引 $I_v = \{(IT_x)_{x\in F}, O_v, O_v'\}$。最终,云服务器存储密文 $IT = \{O_0, O_1, O_2, O_3, IT_x I_v\}$ 进行存储。

(3)生成搜索陷门。Tapdoor(k_u,K_x,g) → td。假设用户关键字集为 $(g_1, g_2, \cdots, g_n) \in U$,用户随机选取 $\zeta \in Z_q^*$,计算 $T_{x,1} = (K_{x,1})^\zeta = g_1^{-ut\zeta}$,$T_{x,2} = (K_{x,2})^\zeta = g_2^{r^2\zeta} \cdot H_1(x)^{uk_x \cdot t \cdot \zeta}$,对关键字 g 加密 $T_v = k^\zeta \cdot H_1(g) = g_2^{r^2\zeta} H_1(g)$。上传并存储陷门 $td = \{T_{x,1}, T_{x,2}, T_v\}$ 到云服务器中。

3.3 解密阶段

解密阶段主要包括用云服务器搜索解密和用户解密两部分。

(1)用云服务器搜索解密。Search&Decrypt(I_v, td,IT_x) → (A_t)。先根据用户提交的搜索陷门验证属性密钥是否满足访问策略,再判断关键字是否能成功匹配。

当不满足访问策略时,算法停止并返回“⊥”。

当满足访问策略时,则存在使 $\sum_{x=1}^{S} \eta_x \cdot v_x = d$ 的一组常数 $\{v_x \in Z_q^*\}_{x\in F}$,云服务器执行外包解密操作,生成部分解密密文 A_t。具体公式如下:

$$A_t = \prod_{x\in S} (e(O_{4,x}, T_{x,1}) e(O_{5,x}, T_{x,2}))^{v_x} =$$

$$\prod_{x\in S} (e(H_1(x)^{uk_x \cdot \eta_x}, g_1^{-ut\zeta}) e(g_1^{u\cdot\eta_x}, g_2^{r^2\zeta} \cdot H_1(x)^{uk_x \cdot t \cdot \zeta}))^{v_x} =$$

$$e(g_1^{u\cdot\eta_x}, g_2^{r^2\zeta})^{v_x} = e(g_1, g_2)^{udr^2\zeta} \quad (3)$$

紧接着云服务器执行搜索计算:

$$A = \frac{e(O_v', T_v)}{A_t} = \frac{e(g_1^{ud}, g_2^{r^2\zeta} H_1(g))}{e(g_1, g_2)^{udr^2\zeta}} =$$

$$e(g_1^{ud}, H_1(g)) \quad (4)$$

先验证 A 与 $O_v = e(g_1^u, H_1(v)^d)$ 是否相等,如果相等,说明搜索成功;否则搜索失败,算法只能终

止并返回“⊥”。

(2) 用户解密。Decrypt(k_u, E_t, IT_0, O_3) → (N)。用户利用 k_u 和 ζ，结合 A_t，对密文 O_3 进行解密，得到明文 N。具体公式如下：

$$N=\frac{O_0\cdot e(O_3,k_1)}{e(O_1,k_2)\cdot A_t^{-\zeta}}=\frac{N\cdot e(g_1,g_2)^{vf}\cdot e(g_1^{f+d},g_2^{ur^2})}{e(g_1^{f},g_2^{v+ur^2})\cdot e(g_1,g_2)^{udr^2}}=N$$

3.4 撤销阶段

撤销属性 x'，属性授权机构生成更新后的密钥，包括属性密钥更新、搜索密钥更新和密文更新三部分。

(1) 属性密钥更新。update_1(x', K_x, $\mathrm{vk}_{x'}$) → (sy_u')。属性授权机构随机选择 $\overline{\overline{\mathrm{uk}}}_{x'}$，计算 $\mathrm{vk}_{x'}=H_1(x)^{(\overline{\overline{\mathrm{uk}}}_{x'}-\mathrm{uk}_{x'})\cdot t}$。输入 $\mathrm{vk}_{x'}$ 和 K_x，计算 $K_{x'}$。进而推得：

$$K_{x,2}'=K_{x,2}\cdot \mathrm{vk}_{x'}=g_2^{r^2}\cdot H_1(x)^{\mathrm{uk}_x\cdot t}\cdot H_1(x)^{(\overline{\overline{\mathrm{uk}}}_{x'}-\mathrm{uk}_{x'})\cdot t}=g_2^{r^2}\cdot H_1(x)^{\overline{\overline{\mathrm{uk}}}_{x'}\cdot t} \tag{5}$$

输出更新后的密钥为：

$$\mathrm{sy}_u'=\begin{cases}k_0=g_1^{r^2},k_1=g_1^{ur^2},k_2=g_1^{v+ur^2},K_{x,1}=g_1^{-ut}\\ \forall x\neq x':K_{x,2}=g_2^{r^2}\cdot H_1(x)^{\mathrm{uk}_x\cdot t}\\ \forall x=x':K_{x,2}'=g_2^{r^2}\cdot H_1(x)^{\overline{\overline{\mathrm{uk}}}_{x'}\cdot t}\end{cases} \tag{6}$$

(2) 搜索密钥更新。update_2(sy_u') → (td')：输入 sy_u'，输出更新后的搜索密钥 td'。更新后的搜索密钥为：

$$\mathrm{td}'=\begin{cases}T_{x,1}=(K_{x,1})^{\zeta}=g_1^{-ut\zeta},T_v=g_2^{r^2\zeta}H_1(g)\\ \forall x\neq x':T_{x,2}=(K_{x,2})^{\zeta}=g_2^{r^2\zeta}\cdot H_1(x)^{\mathrm{uk}_x'\cdot t\cdot\zeta}\\ \forall x=x':T_{x,2}'=(K_{x,2}')^{\zeta}=g_2^{r^2\zeta}\cdot H_1(x)^{\overline{\overline{\mathrm{uk}}}_{x'}\cdot t\cdot\zeta}\end{cases} \tag{7}$$

(3) 密文更新。update_3($\mathrm{vk}_{t'}$, IT_x) → (IT_x')。计算得到 $\mathrm{vk}_{t'}=\frac{\overline{\overline{\mathrm{uk}}}_{x'}}{\mathrm{uk}_x}$，输入 $\mathrm{vk}_{t'}$ 和 IT_x，计算IT_x'。进而推得：

$$O_{4,x}'=(O_{4,x})^{\mathrm{vk}_{t'}}=(H_1(x)^{\mathrm{uk}_x\cdot\eta_x})^{\frac{\mathrm{uk}_x'}{\mathrm{uk}_x}}=H_1(x)^{\overline{\overline{\mathrm{uk}}}_{x'}\cdot\eta_x}$$

输出更新后的属性密文为：

$$\mathrm{IT}_x'=\begin{cases}O_{5,x}=g_1^{u\cdot\eta_x}\\ \forall x\neq x':O_{4,x}=H_1(x)^{\mathrm{uk}_x\cdot\eta_x}\\ \forall x=x':O_{4,x}'=H_1(x)^{\overline{\overline{\mathrm{uk}}}_{x'}\cdot\eta_x}\end{cases} \tag{8}$$

4 安全性与性能分析

4.1 安全性分析

4.1.1 关键字安全

定理 1 若不存在多项式的对手 D 能够通过 TR^* 成功破解本文方案，则 DBDH 困难假设成立，本文方案在关键字攻击下是安全的，通过一个对手 D 和挑战者 T 之间的模拟游戏来证明其安全性。

(1) 初始化：挑战者 T 选取随机数 $\omega\in\{0,1\}$，当 ω 分别等于 0 和 1 时，zz 分别等于 $e(g_1,g_2)^u$ 和 $\mathrm{zz}=e(g_1,g_2)^v$，其中 $u,v\in Z_q^*$。T 执行 setup(ψ) 算法生成 qq 和 zmy，并将 qq 发送给 D，保留 zmy。

(2) 阶段 1：D 根据其属性集 F 自适应向挑战者 C 请求 sy，T 首先检查 F，要求 F 不满足TR^*，随后为每个属性计算 $\mathrm{sy}=\{k_u,K_x\}$，并将计算结果发送给 B。

(3) 挑战：D 发送访问结构 TR^* 以及关键字 g_0 和 g_1 给 T，其中 g_0 和 g_1 长度相等，T 选取随机数 $v\in\{0,1\}$，若 $a=0$，$O_0^*=N\cdot e(g_1,g_2)^{\mathrm{vf}}$；若 $a=1$，$O_0^*=N\cdot e(g_1,g_2)^{\mathrm{wf}}$。$O_1^*=g_1^f$，$O_2^*=g_1^d$，$O_3^*=g_1^{f+d}$，任意 $x\in F$，$O_{4,x}^*=H_1(x)^{\mathrm{uk}_x\cdot\eta_x}$，$O_{5,x}^*=g_1^{u\cdot\eta_x}$，$O_g^*=e(g_1^u,H_1(v)^d)$，$O_g^{*'}=g_1^{\mathrm{ud}}$。关键字索引 $I_g^*=\{(O_{4,x}^*,O_{5,x}^*)_{\forall x\in s},O_g^*,O_g^{*'}\}$，$C$ 生成关键字挑战密文 $\mathrm{IT}^*=\{I_g^*,O_0^*,O_1^*,O_2^*,O_3^*\}$，将 IT^* 返回给 D。

(4) 阶段 2：与阶段 1 完全相同。

(5) 猜测：由于 D 所查询的 F 均不满足TR^*，因此恢复关键字的信息之后，才能区分g_0 和g_1。D 输出 $v=v'$ 的概率为：$\Pr[v=v'\mid a=1]=1/2$。

因此，可以忽略 D 打破 DBDH 问题的优势。

$$\mathrm{Adv}_A^{\mathrm{gjz}}(\varepsilon)=|1/2\Pr[v=v'\mid a=0]+1/2\Pr[v=v'\mid a=1]-1/2|=\left|\frac{1}{2}\times\left(\frac{1}{2}+\varepsilon\right)+\frac{1}{2}\times\frac{1}{2}-\frac{1}{2}\right|=\varepsilon/2$$

4.1.2 陷门安全

定理 2 若 DDH 假设成立，则文中方案在陷门攻击下具有安全性。通过一个对手 D 和挑战者 T 之间的模拟游戏来证明其安全性。

(1) 初始化：与定理 1 中一致，只是此时当 ω 等于 0 和 1 时，zz 分别等于 g_1^u 和 g_1^v。

(2) 阶段 1：与定理 1 中阶段 1 一致。

(3) 挑战：T 选择随机数 b，其中 $b\in\{0,1\}$。D 给 T 提交 2 个关键字g_0 和 g_1，其长度相等，如果 $\omega=0$，则计算 $\mathrm{sy}_u=\{k_0=g_1^{r^2},k_1=g_1^{\mathrm{ur}^2},k_2=g_1^{v+\mathrm{ur}^2},\forall x\in F:K_{x,1}=g_1^{-\mathrm{ut}},K_{x,2}=g_2^{r^2}\cdot H_1(x)^{\mathrm{uk}_x\cdot t}\}$，生成搜索

陷门 $T_v^* = \{T_{x,1}^* = g^{-ut\zeta}, T_{x,2}^* = g_2^{r^2\zeta} \cdot H_1(x)^{\mathrm{uk}_x \cdot t \cdot \zeta}, T_v^* = g_2^{r^2\zeta} H_1(g)\}_{x \in F_u}$,并返回给 D。

(4)阶段 2:此阶段的操作与阶段 1 完全相同。

(5)猜测:D 猜测 τ,当 ω 分别等于 0 和 1 时,T 输出 $\tau = b$ 的概率分别为 $\Pr[\tau = b \mid \omega = 0] = 1/2 + \varepsilon$ 和 $\Pr[\tau = b \mid \omega = 1] = 1/2$。

因此,可以忽略 D 打破 DDH 问题的优势。于是得到:

$$\mathrm{Adv}_A^{\mathrm{xm}}(\varepsilon) = |1/2\Pr[\tau = b \mid \omega = 0] + 1/2\Pr[\tau = b \mid \omega = 1] - 1/2| = \left|\frac{1}{2} \times \left(\frac{1}{2} + \varepsilon\right) + \frac{1}{2} \times \frac{1}{2} - \frac{1}{2}\right| = \varepsilon/2$$

4.1.3 前向安全

当撤销某个用户的属性时,为了及时更新该用户的解密密钥,属性更新密钥 $\mathrm{vk}_{x'}$ 也会被生成,然后分发给没有被撤销的用户。与此同时,云服务器也会利用更新后的密文重新计算 $\mathrm{vk}_{t'}$,并对相关的密文进行重新加密。这种机制确保了旧的解密密钥无法解密更新后的密文,从而实现了前向安全性。

4.1.4 抗合谋攻击

在方案设计中,每个用户都会被分配一个唯一的随机数 t,而属性密钥则是基于用户的属性生成的。尽管存在不同用户属性相同的情况,但随机数 t 是唯一的,并且不同客户的密钥也不完全相同。因此即使用户之间合谋,得不到其他用户的随机数 t,也就无法计算 $K_{x,2}$,从而确保了系统的安全性。

4.2 性能分析

4.2.1 功能对比

将本文提出的方案与文献[1]和文献[13-16]提出的方案在拥有功能方面对比,结果见表 1。

表 1 功能对比

Table 1 Functions comparison

系统属性	文献[13]	文献[14]	文献[15]	文献[16]	文献[1]	本文
细粒度访问	√	√	√	√	√	√
关键字搜索	√	√	√	√	√	√
属性撤销	×	×	×	×	√	√
外包加解密	√	×	×	×	√	√

从表 1 可以看出,文献[14]的访问策略为“AND”门,本文和文献[16]的访问策略为访问树,文献[13]、文献[15]和文献[1]的访问策略都是 LSSS,文献[1]、文献[13-16]与本文方案都支持细粒度访问和关键字搜索,但是文献[13-16]不支持属性撤销,文献[14-16]不支持外包加解密,相比之下本文方案与文献[1]具有优势。

4.2.2 系统性能分析

将本文方案与文献[1]和文献[13-16]提出的方案在系统初始化、密钥生成、加密阶段和搜索阶段四个阶段进行比较。G_1、G_2 和 Z_q 的元素长度分别为 $|G_1|$、$|G_2|$ 和 $|Z_q|$,用户的属性集中属性个数用 f 来表示,e 表示双线性对运算,m 表示哈希计算,h 表示指数运算,w 表示索引中关键字的数量,j 表示访问策略中的属性数量,g 表示用户提交的关键字数量。

存储成本对比见表 2,从表 2 可以看出,初始化阶段时,本文方案与文献[1]、文献[13-16]方案基本相同;在密钥生成阶段,本文方案与文献[1]、文献[14]、文献[16]的方案基本相同,低于文献[13]、[15]的方案;在加密阶段,本文方案低于文献[1]、文献[13-16]的方案;在陷门搜索阶段,本文方案与文献[14-15]基本相同,优于文献[1]、文献[13]和文献[16]的方案。

表 2 存储成本比较

Table 2 Comparison of storage costs

方案	setup	KeyGen	Encrypt	Trapdoor
文献[13]	$(1+f)\lvert G\rvert + f\lvert Z_q\rvert$	$(f+2)\lvert G\rvert + 2\lvert Z_q\rvert$	$(2j+2w+1)\lvert G\rvert + 2\lvert Z_q\rvert$	$(f+2g+3)\lvert G\rvert$
文献[14]	$(4+f)\lvert G\rvert + (2+f)\lvert Z_q\rvert$	$(f+5)\lvert G\rvert$	$\lvert G_0\rvert + (2j+w+4)\lvert G\rvert$	$f\lvert G\rvert + (g+1)\lvert G_0\rvert$
文献[15]	$(2+f)\lvert G\rvert + (4+f)\lvert Z_q\rvert$	$(f+2)\lvert G\rvert + \lvert Z_q\rvert$	$(2j+2w+1)\lvert G\rvert + 2\lvert Z_q\rvert$	$(f+g+2)\lvert G\rvert$
文献[16]	$(1+f)\lvert G\rvert + (3+f)\lvert Z_q\rvert$	$(3f+1)\lvert G\rvert$	$(2j+w+3)\lvert G\rvert + 2\lvert Z_q\rvert$	$(2f+g+2)\lvert G\rvert$
文献[1]	$(2+f)\lvert G\rvert + (3+f)\lvert Z_q\rvert$	$(f+2)\lvert G\rvert$	$(2j+w+2)\lvert G\rvert + \lvert Z_q\rvert$	$(f+2g+1)\lvert G\rvert$
本文	$(3+f)\lvert G\rvert + (2+f)\lvert Z_q\rvert$	$(f+4)\lvert G\rvert$	$(2j+2)\lvert G\rvert$	$(f+g+1)\lvert G\rvert$

计算成本比较见表 3,从表 3 可以看出,在初始化阶段,本文方案与文献[1]、文献[13-16]的方案基本相同;在密钥生成阶段,与文献[13-14]、文献[1]、文献[16]的基本相同,但优于文献[15]的方

案；在加密阶段，低于文献[13-16]的方案；在陷门搜索阶段，与文献[13-14]方案基本相同，略高于文献[15]，略低于文献[1]和文献[16]方案。

表 3　计算成本比较

Table 3　Comparison of calculation cost

方案	setup	KeyGen	Encrypt	Trapdoor
文献[13]	$(2+f)h+(2+f)m$	$(j+2)h+jm$	$(2f+w+1)h+(w+f)m$	$(j+g+2)h+(j+g)m$
文献[14]	$(4+f)h+(2+f)m$	$(j+5)h+jm$	$(2f+w)h+(f+w+4)m$	$(j+g)h+(1+g)m$
文献[15]	$(4+f)h+(4+f)m$	$(2j+2)h+2jm$	$(2f+w+4)h+(w+f+1)m$	$(2+g)h+gm$
文献[16]	$(3+f)h+(3+f)m$	$(j+2)h+jm$	$(2f+6)h+(w+f+2)m$	$(2j+g+2)h+gm$
文献[1]	$(2+f)h+(3+f)m$	$jh+(1+j)m$	$(f+w+5)h+(w+2f)m$	$(2j+g+1)h+(j+g)m$
本文	$(3+f)h+fm$	$(j+1)h+jm$	$(f+w+5)h+(w+f)m$	$(j+g+1)h+(j+g)m$

4.3　实验分析

使用本文的方案进行仿真实验，实验环境为 Windows 64 位操作系统，Intel(R) Core(TM) Ultra 5 125H CPU @ 3.60 GHz，内存 32.0 GB。实验采用 Java 语言在编译工具 IDEA 上完成编译，使用基于双线性配对的密码学库(JPBC)在密钥生成、加密、索引生成以及解密阶段进行实验模拟，本次仿真实验对比了本文所提方案与文献[1]、文献[15]和文献[16]所提方案的计算开销。仿真实验中，属性/关键字个数以 10 为间隔、从 10 个递增到 50 个，为减少实验误差，每组测试进行 1 000 次测算求平均值作为计算结果，实验结果如图 2 所示。

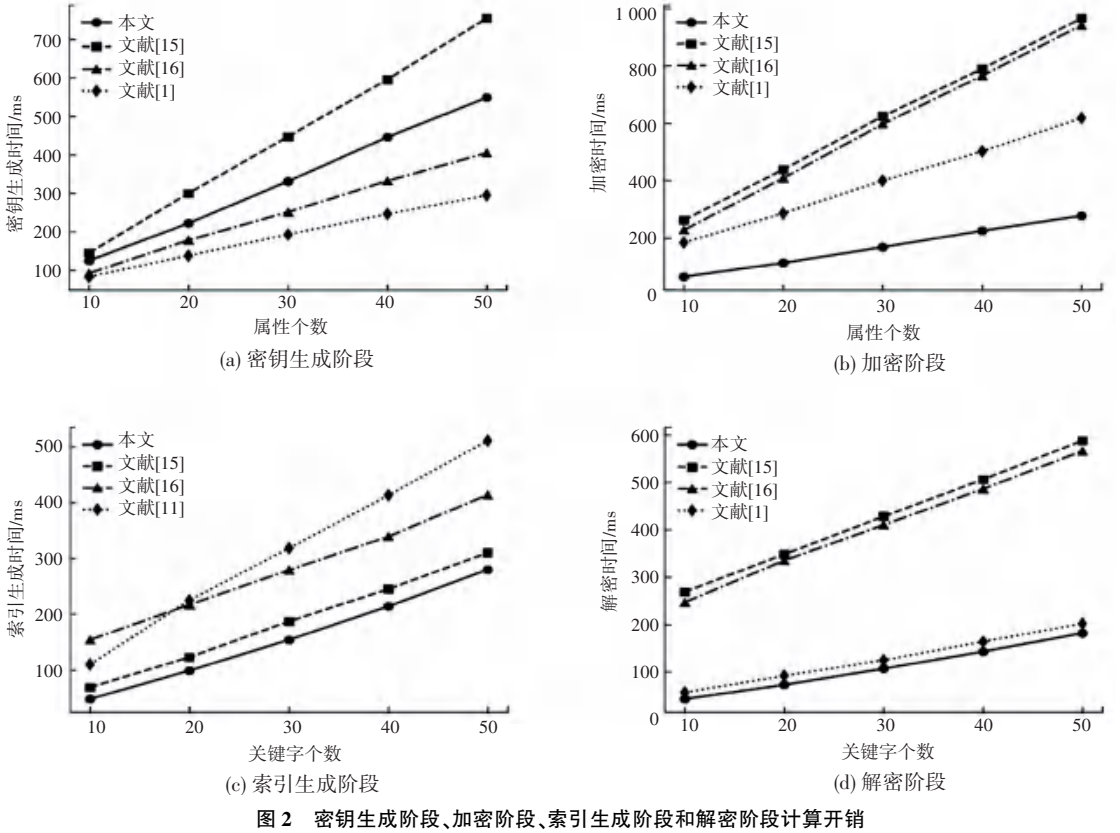

图 2　密钥生成阶段、加密阶段、索引生成阶段和解密阶段计算开销

Fig. 2　Computational overhead of the key generation stage, encryption stage, index generation stage and decryption stage

属性/关键字个数从 10 到 50 时，随着属性个数增加，在密钥生成阶段，由图 2(a)可知，密钥生成时间与属性个数呈现线性相关，与文献[15]相比本文提出的方案为用户生成密钥所花费的时间更短；在 EHR 数据加密阶段见图 2(b)，数据加密时间越长，相比于文献[1]、文献[15-16]，同样的属性个数情况下，本文方案花费时间最短；在索引生成阶段，由图 2(c)可知，本文方案比文献[1]、文献[15-16]所花费

的时间短。在数据解密阶段,从图 2(d)可以看出,相同属性个数的情况下,与文献[1]、文献[15-16]相比,本文方案速度最快。综合来看,本文方案优于文献[1]、文献[15-16]所提方案。

5 结束语

为解决云医疗数据的安全有效共享问题,提出了云医疗中基于非对称配对的属性基可搜索加密方案。该方案通过用结构树构造访问策略,用访问树构造访问策略,非对称配对设置基于属性的可搜索加密,将数据加密、关键字搜索与访问策略相结合,实现了细粒度的数据搜索控制;通过在属性密钥中嵌入版本密钥,结合版本密钥的动态更新机制,实现了密钥与密文的协同更新,确保属性的实时撤销功能得以支持;通过将加解密计算任务外包给云服务器,以此来减轻数据用户和所有者在本地设备的计算负担。安全性分析、性能分析和实验分析的结果表明,本文方案比其他方案功能更多、计算量更少、效率更高,能够在不侵犯患者隐私的情况下有效实现 EHR 数据的安全共享。

参考文献

[1] 唐菊香,李川平,何粒波. 云医疗体系中基于属性加密的数据共享方案[J]. 计算机技术与发展,2024,34(5):205-212.

[2] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]// Proceedings of the 24th Annual International Conference on the Theory and Applications of C-ryptographic Techniques. Cham: Springer, 2005: 457-473.

[3] PIRRETTI M, TRAYNOR P, MCDANIEL P, et al. Secure attribute - based systems [C]//Proceedings of the 13th ACM Conference on Computer and Communications Security. New York: ACM, 2006: 99-112.

[4] LIANG Xiaohui, LU Rongxing, LIN Xiaodong, et al. Ciphertext policy attribute based encryption with efficient revocation [R]. Waterloo, Canada: University of Waterloo, 2010.

[5] OSTROVSKY R, SAHAI A, WATERS B. Attribute - based encryption with non - monotonic access structures [C]// Proceedings of the 14th ACM Conference on Computer and communications security. New York: ACM, 2007: 195-203.

[6] ATTRAPADUNG N, IMAI H. Conjunctive broadcast and attribute-based enc-ryption[C]// Proceedings of the Third International Conference on Pairing - Based Cryptography. Cham: Springer, 2009: 248-265.

[7] MING Yang, HE Baokang, WANG Chenhao. Efficient revocable multi-authority attribute-based encryption for cloud storage[J]. IEEE Access,2021,9:42593-42603.

[8] LIAO Yongjian, HE Yichuan, LI Fagen, et al. Analysis of an ABE scheme with verifiable outsourced decryption[J]. Sensors, 2018,18(1):176.

[9] 周艺华,扈新宇,李美奇,等. 云环境下基于属性策略隐藏的可搜索加密方案[J]. 网络与信息安全学报,2022,8(2):112-121.

[10] MELISSA B, MIGUEL M, HEIDY M. Novel constructions for ciphertext-policy attribute-based searchable encryption[C] // Proceedings of 2022 IEEE Mexican International Conference on Computer Science (ENC). Piscataway,NJ:IEEE,2022:1-8.

[11] 葛江妍,温蜜. 智能电网中高效可撤销的属性基访问控制方案[J]. 计算机应用与软件,2025,42(1):312-318.

[12] XIONG Hu, ZHAO Yannan, PENG Li, et al. Partially policy-hidden attribute-based broadcast encryption with secure delegation in edge computing[J]. Future Generation Computer Systems, 2019,97:453-461.

[13] 李婷,常利伟. 一种可外包解密的高效密文策略的属性基加密方案[J]. 山西大学学报(自然科学版),2022,45(2):387-392.

[14] WU Axin, ZHENG Dong, ZHANG Yinghui, et al. Hidden policy attribute - based data sharing with direct revocation and keyword search in cloud computing[J]. Sensors, 2018, 18(7): 2158.

[15] 薛庆水,时雪磊,王俊华,等. 基于属性加密的个人医疗数据共享方案[J]. 计算机应用研究,2023,40(2):589-594.

[16] 牛淑芬,宋蜜,方丽芝,等. 智慧医疗中基于属性加密的云存储数据共享[J]. 电子与信息学报,2022,44(1):107-117.

[17] 谢小凤,张鑫涛,王鑫,等. 基于云存储的多关键字可搜索加密方案[J]. 信息网络安全,2024,24(9):1444-1457.

[18] 高改梅,张瑾,刘春霞,等. 基于区块链与 CP-ABE 策略隐藏的众包测试任务隐私保护方案[J]. 计算机应用,2024,44(3):811-818.

[19] 陈洪军,景清武,李丹妮,等. 基于 DNA 和对称密码的一次一密加密算法[J]. 智能计算机与应用,2024,14(9):150-154.

[20] 韩磊,刘吉强,韩臻,等. 移动 ad hoc 网络预分配非对称密钥管理方案[J]. 通信学报,2012,33(10):26-34.