文章编号：2095-2163(2023)04-0014-06 中图分类号：TP309.7 文献标志码：A

移动云中支持健康数据共享的可追责大属性多授权 CP-ABE 方案

唐靖蕾，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：在移动医疗健康(mHealth)云中，为实现对个人健康信息(PHR)数据安全共享以及细粒度访问控制，本文提出了一种高效、安全的基于移动健康云的多权限大属性 PHR 访问控制方案。该方案在素数阶群上构造，支持密文在 LSSS 访问结构下加密并与属性相关联，与此同时，将权限泄露给未授权实体的恶意用户放入身份信息表中并精确追踪。在 q-DPBDHE2 假设下，该方案在随机预言模型中被证明具有静态安全性。仿真实验在 Charm 密码框架中实现，与其他方案相比，本文方案具有更好的性能优势以及更高的计算效率。

关键词：属性基加密；可追踪；多授权机构；大属性；访问控制；移动健康

Accountable large-attribute multi-authority CP-ABE scheme for health data sharing in mobile cloud

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

【Abstract】In order to implement attribute-based fine-grained access control for Personal Health Information (PHR) in Mobile Health (mHealth) cloud, this paper proposes an efficient and secure multi-privilege and large-attribute PHR access control scheme based on mHealth cloud. The scheme is constructed on the prime order group, and the ciphertext is encrypted under the LSSS access structure and associated with attributes. At the same time, the malicious users who leaked their permissions to unauthorized entities are put into the identity information table and accurately tracked. Under the q-DPBDHE2 assumption, the scheme is proved to be statically secure in the random oracle model. The simulation experiment is implemented in the Charm cryptographic framework. Compared with other schemes, the proposed scheme has better performance advantages and higher computational efficiency.

【Key words】attribute-based encryption; accountability; multi-authority; large attribute; access control; mHealth

0 引 言

移动健康医疗(mHealth)云集合了广泛的新兴技术[1]，如可穿戴医疗传感器、云计算、通信技术。移动健康系统使患者能够通过各种可穿戴或可植入的医疗物联网传感器监测和收集人体信息，并通过移动设备集成个人健康记录(PHR)。然后，PHR 将通过 5G 网络上传到云服务器，以节省移动设备的有限存储容量。由于 PHR 数据包含各种隐私信息，持有者希望实施访问控制策略以确保 PHR 数据只能由授权用户访问。然而，如果采用传统的访问控制技术，则由于云服务器无法完全信任或仅支持粗粒度访问策略，PHR 数据安全将会受到损害。

为了解决上述问题，基于密文策略属性的加密(CP-ABE)[2]被提出，该技术可以同时实现细粒度访问控制和数据安全。在 CP-ABE 中，密文中加入访问策略，用户的私钥由属性集创建。只有当用户的属性集与嵌入的访问策略匹配时，解密才会成功。尽管传统的 CP-ABE 机制可以保护敏感 PHR 数据的安全性和隐私性，防止泄露给未经授权的用户，但

基金项目：国家自然科学基金(61941205)。
作者简介：唐靖蕾(1998-)，女，硕士研究生，主要研究方向：云数据安全；巫朝霞(1975-)，女，博士，教授，硕士生导师，主要研究方向：信息安全研究。
通讯作者：巫朝霞 Email：wuzhaoxia828@163.com
收稿日期：2022-12-09

在 mHealth 中广泛部署和应用之前，仍有 2 个主要的挑战性问题需要进行探讨与研究。

首先，传统的 ABE 的目标是实现“一对多”的加密，但单一权限和属性的分散管理问题是其实现的瓶颈，因此需要在分布式系统中使用多权限 ABE 设计。针对这些问题，Chase[3] 提出了最初的多权威 ABE（MA-ABE）方案，其中存在一个中央权威（CA）和多个属性权威（AA），每个用户都用唯一的全局标识符（gid）标记。随后，MA-ABE 出现了多种增强和扩展。Lewko 等学者[4] 提出了去中心化多授权机构 CP-ABE 方案，该方案在随机预言机模型下被证明是完全安全的。Zhang 等学者[5] 提出了基于匿名认证的个人健康记录的 MA-ABE，在用户与云服务器之间进行认证时隐藏用户的身份和属性。

然而，在实际中移动健康云需要对属性和用户进行动态扩容，因此大属性 ABE 比小属性 ABE 更实用。在小属性框架中，所选安全参数的属性集被限制为多项式大小。这一限制将对移动健康云中的动态实际应用造成瓶颈。在大型属性集系统中，属性域可以设为指数级大。Rouselakis 等学者[6] 在素数阶双线性群中构造了一个大属性 MA-ABE 方案，该方案比复合阶双线性群效率更高。Huang[7] 基于素数阶双线性群，提出了第一个无密钥滥用的可撤销大属性去中心化 MA-ABE，该方案支持属性、用户和权限的动态扩展，但其访问结构存在暴露风险。

其次，文献[3-7]中的方案只考虑多授权机构的问题，但未能考虑恶意用户追踪问责等问题，为实现叛徒可追踪，需防止合法用户密钥滥用。Liu 等学者[8] 提供了一个高度表达的白盒跟踪方案，支持任何单调访问策略。Zhou 等学者[9] 提出支持白盒跟踪和撤销的 MA-ABE，应用于电子医疗云计算系统的多层隐私保护，只实现数据用户身份的隐私，但系统需要大量的计算消耗。

本文在文献[6]的基础上，结合追踪算法[10] 提出了一种面向移动健康支持大属性多授权机构的可追踪 CP-ABE 方案，该方案的特点如下：

(1)支持属性、用户和权限的动态扩容，适用于动态移动健康系统中大规模的多领域协作。

(2)根据追踪算法可以检验出参与泄露解密密钥的恶意用户，从而提高了效率，并且不需要存储开销。

(3)线性秘密共享方案提供了按需求频繁地修改密文访问策略的灵活性，允许对数据所有者进行研究细粒度控制。

1　背景知识

1.1　双线性映射

设 G_0、G_1、G_T 都是阶为素数 p 的乘法循环群，双线性映射 $e: G_0 \times G_1 \rightarrow G_T$ 具备以下 3 个特性：

(1)双线性：对于 $\forall a,b \in Z_p$，$\forall u \in G_0$，$\forall v \in G_1$，有 $e(u^a,v^b) = e(u,v)^{ab}$，当 $G_0 = G_1$ 时称为对称双线性映射。

(2)非退化性：$\exists u,v \in G_0$，使得 $e(u,v) \neq 1$。

(3)可计算性：对于 $\forall u,v \in G_0$，可以有效计算 $e(u,v)$。

1.2　线性秘密共享方案(LSSS)

假设 $\mathbb{A}$ 是一个单调的访问结构，$\boldsymbol{M}$ 是一个 $l \times k$ 的矩阵，ρ 是一个行标记函数：将 $\boldsymbol{M}$ 中的行 i 映射为 $\mathbb{A}$ 中的属性 $att(i)$。一个 LSSS 由 2 个多项式时间的算法组成：

(1)共享算法 $((\boldsymbol{M},\rho),s)$：该算法输入 $(\boldsymbol{M},\rho)$ 和一个秘密值 $s \in \mathbb{Z}_p$，并随机选取元 $r_2,r_3,\cdots,r_n \in \mathbb{Z}_p$，设定向量 $\vec{v} = (s,r_2,r_3,\cdots,r_n) \in \mathbb{Z}_p^k$。该算法输出一个集合作为 s 的共享份额，其中 $\vec{M}_i \in \mathbb{Z}_p^k$ 是矩阵 $\mathbb{M}$ 的第 i 行，共享份额 $\lambda_{\rho(i)}$ 属于属性 $\rho(i)$。

(2)重构算法 $((\boldsymbol{M},\rho),L)$：该算法输入 $(\boldsymbol{M},\rho)$ 和一个授权属性集合 $L \in \mathbb{A}$。该算法输出一个秘密重构系数集合 $\{\omega_i\}_{i \in I} \subset \mathbb{Z}_p$ 使得 $\sum_{i \in I} \omega_i \vec{M}_i = (1,0,\cdots,0)$，$I = \{i \in [l]: \rho(i) \in L\}$。因此有 $\sum_{i \in I} \omega_i \lambda_{\rho(i)} = s$。

1.3　困难假设

判定性 q-BDHE2（q-Decisional Parallel Bilinear Diffie-Hellman Exponent 2，q-DPBDHE2）假设[6]，即：

给定 $\mathbb{G}$ 和 $\mathbb{G}_T$ 为素数阶 p 的双线性群，g 为 $\mathbb{G}$ 的一个生成元。$e: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ 是一个定义在 $\mathbb{G}$ 上的双线性映射。随机选取 $s,a,b_1,b_2,\cdots,b_q \in Z_p^*$，$R \in \mathbb{G}_T$，给定 $D = \{G,p,e,g,g^s,g^{a^i},g^{a^i b_j},i \in [2q],j \in [q],i \neq q+1,g^{sa^i b_j/b_{j'}},i \in [q+1],j \in [q],j' \in [q],j \neq j'\}$，并要求从 (D,R) 区分 $(D,e(g,g)^{sa^{q+1}})$。算法 A 用求解 G 群中的 q-DPBDHE2 问题的优势：$|\Pr[A(D,e(g,g)^{sa^{q+1}}) = 0] - \Pr[A(D,R) = 0]| \geqslant \varepsilon$。

如果不存在概率多项式时间算法以不可忽略的优势解决判定性 q-BDHE2 问题，则称 q-BDHE2 问题是困难的。

2 方案构造

2.1 系统模型

本次研究的方案构造模型如图 1 所示。方案中主要实体包括:属性授权机构(Attribute Authority, AA)、移动健康云服务提供商(mHealth Cloud Service Provider, mCSP)、数据持有者(Data Owner, DO)、数据用户(Data User, DU)。

对个人健康记录(PHR)数据共享模型中的实体介绍如下:

(1)AA 是属性授权机构,每个属性权威拥有并管理一个属性集合,各个属性权威所管理的属性集合不存在交集。

(2)mCSP 是系统中可提供强大的存储能力和通信能力的云服务商,主要负责系统中 PHR 存储、管理密文数据和关键词搜索等服务。

(3)DO 是指数据的持有者,通过移动或可穿戴物联网设备收集和集成 PHR,数据持有者希望将其数据外包到 mCSP 提供给云中的客户。

(4)DU 是指访问云中数据的用户,例如医生、营养师、研究人员等。每个数据用户都有自己的私钥与自己的属性集相关联。

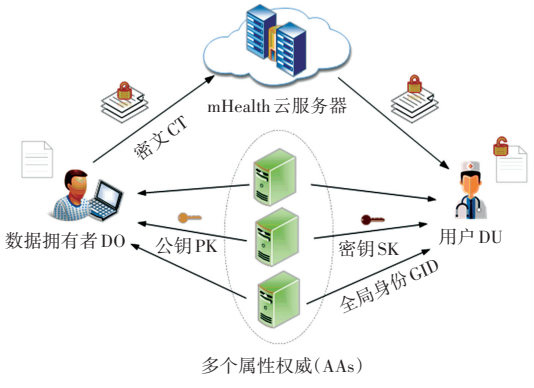

图 1 本文方案构成

Fig. 1 The scheme proposed in the paper

2.2 具体方案

在本方案的构造中,U 是属性集合,U_θ 是权威机构集合,对于每个属性 $i \in U$ 由特定的权威 θ 控制,一个公共可计算函数 $T: U \to U_\theta$ 将属性 i 映射到权威 θ,对于 $l \times n$ 访问矩阵 $\boldsymbol{A}$,ρ 将其行映射到属性,函数 $\delta(\cdot) = T(\rho(\cdot))$ 将其行映射给权威机构。假设 $\mathbb{G}$ 是素数阶 p 的双线性群,$e: G \times G \to G_T$ 是一个双线性映射。对此拟展开研究分述如下。

(1) Global Setup(λ) $\to GP$。算法中,首先选择阶为素数 p 的双线性群,g 是 $\mathbb{G}$ 的生成元,$e: \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ 是 $\mathbb{G}$ 双线性映射,然后将选择哈希函数 $H: Z_p^* \to \mathbb{G}$ 将用户身份映射到 $\mathbb{G}$ 群的元素,哈希函数 $F: U \to \mathbb{G}$ 将用户属性映射到群 $\mathbb{G}$ 的元素,全局公共参数为:

$$GP = \{p, G, g, H, F, U, U_\theta, T\} \tag{1}$$

(2) Authority Setup(GP) $\to PK_\theta, MSK_\theta$。每个权威 $\theta \in U_\theta$ 选择 3 个随机指数 $\alpha_\theta, y_\theta, a_\theta \in Z_p^*$,并计算公钥 $PK_\theta = \{e(g,g)^{\alpha_\theta}, g^{y_\theta}, g^{a_\theta}\}$ 和私钥 $SK_\theta = \{\alpha_\theta, y_\theta, a_\theta\}$。身份标识表 L 被初始化为空表。

(3) $Encrypt(GP, M, \mathbb{A}, \{PK_\theta\}) \to CT$。给出明文 M,访问策略 $(\mathbb{A}, \rho)$,相关属性公钥 $\{PK_\theta\}$,算法首先选择 2 个随机向量 $v = (s, v_2, \cdots, v_n)^{\mathrm{T}}$,$\omega = (0, \omega_2, \cdots, \omega_n)^{\mathrm{T}} \in Z_p^n$,对于每个 $x = \{1, 2, \cdots, l\}$,计算 $\lambda_x = A_x \cdot v$,$\omega_x = A_x \cdot \omega$,其中 A_x 是 $\mathbb{A}$ 的第 x 行,算法选择随机数 $r_x \in Z_p$,计算密文 CT 如下:

$$C_0 = Me(g,g)^s, C_1 = e(g,g)^{\lambda_x} e(g,g)^{\alpha_{\delta(x)} r_x}, C_2 = g^{-r_x}, C_3 = g^{y_{\delta(x)} r_x} g^{\omega_x}, C_4 = F(\rho(x))^{r_x}, C_5 = g^{-a_{\delta(x)} r_x}$$

(4) $KeyGen(GP, ID, S, \{MSK_\theta\}) \to SK$。输入全局参数 GP,身份 ID,属性集 S,以及相关权威的主密钥 $\{MSK_\theta\}$,对于每个属性 $i \in S$,如果 $T(i) = \theta$,权威机构 θ 选择 2 个随机值 $t \in Z_p$,计算 $K_1 = g^{\frac{\alpha_\theta}{a_\theta + ID}} H(ID)^{\frac{y_\theta}{a_\theta + ID}} F(i)^t, K_2 = g^t, T_1 = ID, T_2 = g^{a_\theta t}$。

属性集 S 的 GID 私钥:$SK_u = \{K_1, K_2, T_1, T_2\}$,算法把 (K_2, ID) 放入身份信息表 L,其中 K_2 关联用户身份 ID 并作为追踪参数。

(5) $Decrypt(GP, CT, SK) \to M$。给定公共参数 GP,密钥 SK_u,密文 CT,$I \subset \{1, 2, \cdots, l\}$ 定义为 $I = \{x: \rho(x) \in S\}$,如果 S 不满足访问策略 (A, ρ),输出 $\perp$。否则对于每个 $x \in I$,算法首先计算 $D_x = C_1 e(K_1, C_2^{T_1} C_5)\, e(H(T_1), C_3)\, e(K_2^{T_1} T_2, C_4)$;然后,计算常数 $\{c_x \in Z_p\}_{x \in I}$,使 $\sum_{x \in I} c_x A_x = (1, 0, \cdots, 0)$,计算得出 $\prod_{x \in I} D_x^{c_x} = e(g,g)^s$;最后,可以将消息恢复为 $M = C_0 / e(g,g)^s$。

(6) Key Sanity Check(GP, SK_u) $\to$ 1 or 0。输入公共参数 GP 和私钥 SK_u,算法将检查解密密钥是否满足完整性检查,该检查由 3 个部分组成:

① $K_1, K_2, T_2 \in G, T_1 \in Z_p^*$。

② $e(g, T_3) = e(K_2, g^{a_\theta})$。

③ $e(K_1, g^{a_\theta} g^{T_1}) = e(g,g)^{\alpha_\theta} e(H(T_1), g^{y_\theta})\, e(F(i), T_2)^{iT_1}$。

如果解密密钥 SK_u 满足式①、②、③,则可以通

过密钥完整性检查，算法输出 1；否则，算法输出 0。

(7) $Trace(GP, \{PK_\theta\}, SK_u, L) \rightarrow ID$。该算法由权威机构执行。如果解密密钥$SK_u$不能通过密钥完整性检查，算法中止，输出 $\perp$。如果 SK 是正常结构的，则算法在表 L 中查找K_2：如果能够在 T 中找到 K_2，则算法输出相应的 id，否则算法输出 $\perp$，表示该私钥未被系统分发。

3　方案分析

3.1　正确性证明

由用户执行 $Decrypt()$ 算法，当用户的属性满足访问机构的设定，才能正确解密出密文，本文方案的正确性证明如下：

$$D_x = C_1 e(K_1, C_2^{T_1} C_5)\, e(H(T_1), C_3) e(K_2^{T_1} T_2, C_4) = e(g,g)^{\lambda_x} e(g,g)^{\alpha_\theta r_x}$$

$$e(g^{\frac{\alpha_\theta}{a_\theta + ID}} H(ID)^{\frac{y_\theta}{a_\theta + ID}} F(i), g^{-r_x ID} g^{-a_\theta r_x}) e(H(ID), g^{y_\theta r_x} g^{\omega_x}) e(g^{tID} g^{a_\theta t}, F(i)^{r_x}) = e(g,g)^{\lambda_x} e(g,g)^{\alpha_\theta r_\theta} e(g,g)^{-r_x \alpha_x} e(g, H(ID))^{-r_x y_x} e(F(i)^t, g^{-r_x(ID + a_\theta)}) \cdot e(H(ID), g)^{y_\theta r_x} e(H(ID), g)^{\omega_x} e(g, F(i))^{r_x t(ID + a_\theta)} = e(g,g)^{\lambda_x} e(H(ID), g)^{\omega_x}$$。

如果属性集合 S 满足访问策略 (A, ρ)，计算常数 $\{c_x \in Z_p\}_{x \in I}$ 使 $\sum_{x \in I} c_x A_x = (1,0,\cdots,0)$，然后得到 $\sum_{x \in I} \lambda_x c_x = \sum_{x \in I} A_x \cdot v \cdot c_x = v \cdot (1,0,\cdots,0) = s$，$\sum_{x \in I} \omega_x c_x = \sum_{x \in I} A_x \cdot \omega \cdot c_x = \omega \cdot (1,0,\cdots,0) = 0$。因此，

$$\prod_{x \in I} D_x^{c_x} = \prod_{x \in I} (e(g,g)^{\lambda_x} e(H(ID), g)^{\omega_x})^{c_x} = e(g,g)^{\sum_{x \in I} \lambda_x c_x} e(H(ID), g)^{\sum_{x \in I} \omega_x c_x} = e(g,g)^s$$

最后得到 $C_0 / (\prod_{x \in I} D_x^{c_x}) = M$。

3.2　安全性证明

定理 1 证明了所提出的方案如同文献[6]方案一样是静态安全的。

定理 1　在 q-DPBDHE2 假设下，提出的具体方案在随机预言模型中是静态安全的。

证明　假设存在一个概率多项式时间敌手 B，该 A 能以不可忽略的优势 ε 攻破所提出的方案，那么可以构建一个模拟器 B，以同样的优势 ε 攻破文献[8]方案。用 C 表示文献[8]方案的挑战者。接下来展开研究分述如下。

(1)全局设置。B 从 C 获取全局参数 $GP = \{p, G, g, H, F, U, U_\theta, T\}$，然后将其传递给敌手 A。

(2)敌手查询。敌手 A 静态地发出多项式有限数量的查询。

(3)授权机构的公钥查询。敌手 A 提交一组没有腐败的属性集合 $N_\theta \in U_\theta$ 和一组腐败属性集合 $C_\theta \in U_\theta, N_\theta \cap C_\theta = \emptyset$。在文献[8]方案中创建其对应的公钥为 $\{PK'_\theta\}_{\theta \in C_\theta}$，对于 $\theta \in C_\theta$，敌手 A 选择 2 个随机数 $a_\theta, b_\theta \in Z_p^*$，并将本文中腐败权威的公钥设为 $\{PK_\theta = PK'_\theta, g^{a_\theta}, g^{b_\theta}\}$。

(4)用户的属性密钥查询。敌手 A 根据用户自身的 id 创建密钥 SK_u，并提交一串序列 $\{(ID_j, S_j)\}_{j=1}^m$，表示敌手查询与用户 ID_j 相关属性集合 S_j 的密钥。

(5)加密查询。敌手 A 提交访问结构 (A, ρ)，和 2 个同等长度明文 m_0, m_1。设 S_{C_θ} 是腐败权威控制的所用属性的集合，$j \in [m]$，要求集合 $S_{C_\theta} \cup S_j$ 不满足 (A, ρ)。

(6)挑战者回复。C 随机选择 $b \in 0,1$，对查询的响应如下：

在接收到敌手的查询后，模拟器 B 发送 $C_\theta, N_\theta, \{PK'_\theta\}_{\theta \in C_\theta}, \{(ID_j, S_j)\}_{j=1}^m, (A, \rho), m_0, m_1$ 给 C 请求提供相应的文献[8]里的公钥、密钥、挑战密文。然后 C 返回公钥 $PK'_\theta = \{e(g,g)^{\alpha_\theta}, g^{y_\theta}\}$，私钥 $\{SK_u{}' = (g^{\alpha_\theta} H(ID_j)^{y_\theta} F(i)^t, g^t)_{i \in S_j}\}$，$j \in [m]$，挑战密文 CT' 如下：

$$C_0 = M_b e(g,g)^s,\ C_1 = e(g,g)^{\lambda_x} e(g,g)^{\alpha_{\delta(x)} r_x},\ C_2 = g^{-r_x},\ C_3 = g^{y_{\delta(x)} r_x} g^{\omega_x},\ C_4 = F(\rho(x))^{r_x}$$

其中，$x = 1,2,\cdots,l$，然后 B 以如下方式回复查询。

(7)授权机构的公钥回复。对于每个权威 $\theta_n \in N_\theta$，B 随机选择 $a_\theta, b_\theta \in Z_p^*$，假设公钥 $PK_\theta = \{e(g,g)^{\alpha_\theta}, g^{y_\theta}, g^{a_\theta}\}$。

(8)用户的密钥回复。$j \in [m], i \in S_j$，B 随机选择 r，设置 $t' = \frac{t}{a_\theta + ID}$，计算 $K_{1,i} = (g^{\alpha_\theta} H(ID_j)^{y_\theta} F(i)^t)^{\frac{1}{a_\theta + ID}} = g^{\frac{\alpha_\theta}{a_\theta + ID_j}} H(ID_j)^{\frac{y_\theta}{a_\theta + ID_j}} F(i)^{t'}$，$K_{2,i} = (g^t)^{\frac{1}{a_\theta + ID_j}} = g^{t'}$，$T_{1,i} = ID_j, T_{2,i} = K_{2,i}^{a_\theta} = g^{a_\theta \frac{t}{a_\theta + ID_j}} = g^{a_\theta t'}$，$B$ 选择另一个随机值 r，再次尝试回复，最后 B 将密钥设置为：$SK_{S_j, ID_j} = \{K_{1,i}, K_{2,i}, T_{1,i}, T_{2,i}\}_{i \in S_j}$。

(9)加密回复。对于 $x \in \{1,2,\cdots,l\}$，B 计算 $C_{5,x} = C_{2,x}^{a_{\delta(x)}} = g^{-a_{\delta(x)} r_x}$，$B$ 设定挑战密文 $CT = (C_0, \{C_{1,x}, C_{2,x}, C_{3,x}, C_{4,x}, C_{5,x}\}_{x \in \{1,2\cdots,l\}})$，最后 B 发送公钥 $\{PK_\theta\}_{\theta \in N_\theta}$，密钥 $\{SK_{S_j, ID_j}\}_{j=1}^m$ 和挑战密文 CT 给敌手 A。

在猜测阶段中，A 输出一个猜测 $b' \in \{0,1\}$，如果 $b' = b$，则 A 赢得游戏。

如果 A 有优势 $AdvA(\lambda) = \varepsilon$ 在破坏本文方案时，B 可以以相同的优势 $AdvA(\lambda) = \varepsilon$ 破坏文献[6]方案，参见方案文献[6]。在 q-DPBDHE2 假设下，文献[6]方案在随机预言模型中是静态安全的，因此本文提出的方案也是静态安全的。

3.3 性能分析

本方案与文献[6]、文献[11]、文献[12]进行了性能比较，主要是从方案的访问结构，可追踪性等 6 个方面，分别对相关多授权机构方案进行对比分析。其中，符号及对应含义见表 1。在本次研究的效率比较中，只考虑成本高的操作。

表 2 给出了相关多授权机构方案的特征比较。从表 2 可以看出，文献[11]采用阈值访问结构，与本文方案采用的 LSSS 访问结构相比灵活性更差。文献[12]采用合数阶群，而本文方案基于素数阶群上的构造，从而具有更好的执行效率。从整体功能上看，本文提出的方案同时支持多个授权机构、大属性以及恶意用户追踪，因此，该方案相比文献[6]的方案具有更丰富的功能。

表 1 符号及对应含义

Tab. 1 Symbols and corresponding meanings

符号	含义
P	双线性配对运算需要的时间
E	G_1 中幂运算需要的时间
$\hat{Ee}$	G_T 中幂运算需要的时间
l	访问策略的复杂度
n	权威机构属性个数

计算复杂度比较见表 3。从表 3 可以看出，对比文献[6]，本文方案为实现可追踪的功能，多进行了一个指数运算，即在群 G_1 上指数运算增加了 1，但总体的加密、解密时间和文献[6]方案的差距不大。本文方案的加密时间比文献[11]方案的更优，文献[11]在加密阶段使用多次双线性配对运算，导致加密时间增加。本文方案和文献[6]、文献[12]都是基于 LSSS 提出的，但只有本文和文献[6]方案支持大属性，因此属性全集在系统建立阶段不需要具体化，属性个数可以无限增多，在加密、解密上都能快速运算。在解密开销方面，本文方案还远远优于文献[12]方案。

表 2 方案功能特征对比

Tab. 2 Comparison of the functional characteristics of the schemes

方案	访问结构	大属性	多授权机构	可追踪性	群阶数	安全模型
文献[6]	LSSS	√	√	×	素数阶	随机预言模型
文献[11]	Threshold	×	√	×	素数阶	标准模型
文献[12]	LSSS	×	√	×	复合阶	随机预言模型
本文方案	LSSS	√	√	√	素数阶	随机预言模型

表 3 计算复杂度比较

Tab. 3 Computational complexity comparison

方案	加密时间	解密时间
文献[6]	$(2l+1)P + 4E + 3E\hat{e}$	$(3+l)P + 2lE$
文献[11]	$(4n+2nl)E + nP$	$2(n+1)nP$
文献[12]	$2P + 2E\hat{e} + (n+4)E$	$(3n+3)P + (3n+1)E\hat{e}$
本文方案	$(2l+1)P + 5E + 3E\hat{e}$	$(3l+1)P + (2l+1)E$

为了衡量本文方案与文献[6]、文献[11]中所提方案的加解密开销，本方案所有仿真实验都在配置为 Intel(R) Core(TM) i5-11300H@3.10 GHz，RAM 为 16 GB 的 Windows10 系统笔记本电脑上的虚拟机运行，虚拟机平台：VMware ® Workstation 16Pro，操作系统为 Ubuntu20.04。本实验利用 Python 语言进行编译，算法仿真中双线性对的选择基于超奇异对称椭圆曲线组(SS512)，仿真结果取 50 次测试结果的平均值。

不同方案加密时间比较如图 2 所示，不同方案解密时间比较如图 3 所示。由图 2、图 3 可知，加密、解密随着属性的数量呈线性增长。从图 2 可以

看出，所提方案的加密时间与文献[6]方案几乎相同，都低于文献[11]方案。在图 3 中，很容易看出，提出的方案比文献[8]方案需要更多的解密时间，但明显低于文献[11]方案的解密开销。

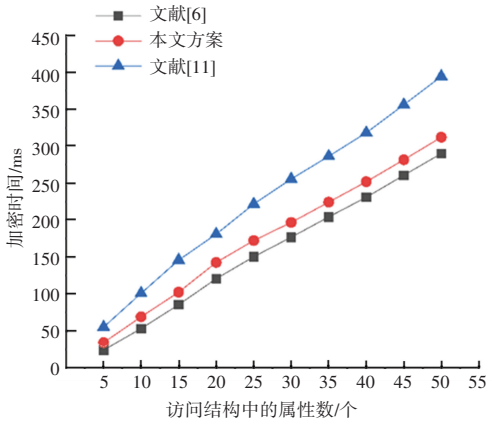

图 2　不同方案加密时间比较

Fig. 2　Comparison of encryption time of different schemes

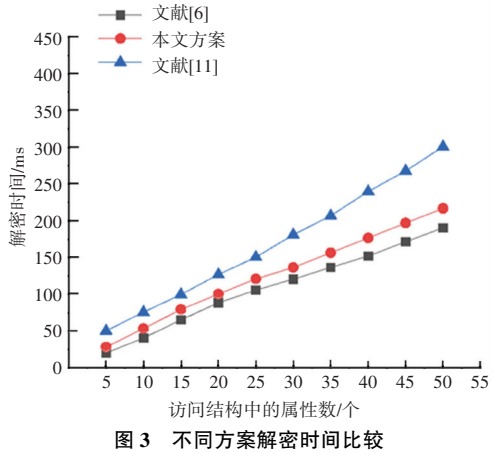

图 3　不同方案解密时间比较

Fig. 3　Comparison of decryption time of different schemes

4　结束语

本文根据移动健康的应用提出一种大属性域可追责的多权威机构属性加密方案，方案减少了中央权威的负荷和风险；采用 LSSS 访问结构，使访问策略具有高表达力和高拓展性；在 q-DPBDHE2 假设下，该方案在随机预言模型中是静态安全的。实验结果和性能分析显示，本文方案在加解密效率上优于对比方案，且在功能上更丰富。

参考文献

[1] LI Qi, ZHU Hongbo. Multi-authority attribute-based access control scheme in mhealth cloud with unbounded attribute universe and decryption outsourcing[C]//2017 9th International Conference on Wireless Communications and Signal Processing (WCSP). Nanjing: IEEE, 2017: 1-7.

[2] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption [C]//2007 IEEE Symposium on Security and Privacy (SP'07). Berkeley, CA, USA: IEEE, 2007: 321-334.

[3] CHASE M. Multi-authority attribute based encryption [C]// Theory of Cryptography Conference. Berlin/ Heidelberg: Springer, 2007: 515-534.

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

[5] ZHANG Leyou, YE Yadi, MU Yi. Multiauthority access control with anonymous authentication for personal health record [J]. IEEE Internet of Things Journal, 2020, 8(1): 156-167.

[6] ROUSELAKIS Y, WATERS B. Efficient statically-secure large-universe multi-authority attribute-based encryption [C]// International Conference on Financial Cryptography and Data Security. Berlin/ Heidelberg: Springer, 2015: 315-332.

[7] HUANG Kaiqing. Revocable large universe decentralized multi-authority attribute-based encryption without key abuse for cloud-aided IoT[J]. IEEE Access, 2021, 9: 151713-151728.

[8] LIU Zhen, CAO Zhenfu, WONG D S. White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures[J]. IEEE Transactions on Information Forensics and Security, 2012, 8(1): 76-88.

[9] ZHOU Jun, CAO Zhenfu, DONG Xiaolei, et al. TR-MABE: White-box traceable and revocable multi-authority attribute-based encryption and its applications to multi-level privacy-preserving e-healthcare cloud computing systems [C]//2015 IEEE Conference on Computer Communications (INFOCOM). Hong Kong, China: IEEE, 2015: 2398-2406.

[10] WANG X, WANG G, XU Y, et al. Traceable ciphertext policy attribute-based encryption scheme with user revocation for cloud storage[J]. Journal of Electronics and Information Technology, 2018, 40(4): 802-810.

[11] ZHANG Leyou, REN Juan, MU Yi, et al. Privacy-preserving multi-authority attribute-based data sharing framework for smart grid[J]. IEEE Access, 2020, 8: 23294-23307.

[12] YANG Yan, CHEN Xingyuan, CHEN Hao, et al. Improving privacy and security in decentralizing multi-authority attribute-based encryption in cloud computing[J]. IEEE Access, 2018, 6: 18009-18021.