mHealth 中可追踪多授权机构基于属性的访问控制方案

李琦[1,2,3]，朱洪波[2,4]，熊金波[5]，莫若[6]

（1. 南京邮电大学计算机学院、软件学院、网络空间安全学院，江苏 南京 210023；
2. 南京邮电大学物联网技术与应用协同创新中心，江苏 南京 210003；
3. 南京邮电大学江苏省大数据安全与智能处理重点实验室，江苏 南京 210023；
4. 南京邮电大学通信与信息工程学院，江苏 南京 210003；5. 福建师范大学数学与信息学院，福建 福州 350117；
6. 西安电子科技大学网络与信息安全学院，陕西 西安 710071）

摘 要：移动健康护理作为一种新兴的技术给个人健康档案的分享提供了极大的便利，也给其隐私带来了极大的风险。基于属性的加密体制能够对加密数据实现细粒度的访问控制，有效地保护了个人健康档案的隐私。然而，目前基于属性的访问控制方案要么缺乏有效的恶意用户追踪机制，要么只支持单个授权机构。针对该问题，提出了一个移动健康护理环境下适应性安全的可追踪多授权机构基于属性的访问控制方案，该方案在合数群上构造，支持任意单调的线性秘密共享机制的访问策略，基于子群判定假设证明了该方案在标准模型下是适应性安全的，基于 *k*-SDH 假设证明了该方案的可追踪性，性能分析表明了该方案的实用性。

关键词：属性加密；多机构；可追踪；适应性安全；移动健康护理

中图分类号：TP309

文献标识码：A

doi: 10.11959/j.issn.1000-436x.2018100

Multi-authority attribute-based access control system in mHealth with traceability

LI Qi[1,2,3], ZHU Hongbo[2,4], XIONG Jinbo[5], MO Ruo[6]

1. School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China
2. Jiangsu Innovative Coordination Center of Internet of Things, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
3. Jiangsu Key laboratory of Big Data Security & Intelligent Processing, Nanjing University of Posts and Telecommunications, Nanjing 210023, China
4. College of Telecommunications & Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
5. College of Mathematics and Informatics, Fujian Normal University, Fuzhou 350117, China
6. School of Cyber Engineering, Xidian University, Xi'an 710071, China

Abstract: Mobile healthcare (mHealth) is an emerging technology which facilitates the share of personal health records (PHR), however, it also brings the risk of the security and privacy of PHR. Attribute-based encryption (ABE) is regarded as a new cryptology to enhance fine-grained access control over encrypted data. However, existing attribute-based mHealth systems either lack of efficient traceable approach, or support only single authority. A traceable multi-authority attribute-based access control mHealth scheme was proposed, which was constructed over composite order groups and supports any monotonic access structures described by linear secret sharing scheme (LSSS). The adaptive security was proved under subgroup decisional assumptions. The traceability was proved under *k*-strong Diffie-Hellman (*k*-SDH) assumption. The performance analysis indicates that the proposed scheme is efficient and available.

Key words: attribute-based encryption, multi-authority, traceable, adaptively secure, mHealth

---

收稿日期：2017-10-02；**修回日期**：2018-05-08

基金项目：国家自然科学基金资助项目（No.61502248, No. 61427801, No.61402109, No.61602365, No.61370078）；中国博士后科学基金资助项目（No.2018M632350）；南京邮电大学引进人才科研启动基金资助项目（No.NY215008）

Foundation Items: The National Natural Science Foundation of China (No.61502248, No.61427801, No.61402109, No.61602365, No.61370078), The Postdoctoral Science Foundation Project of China (No.2018M632350), NUPTSF (No.NY215008)

1 引言

移动健康（mHealth, mobile healthcare）护理系统[1]经由移动设备，集合了各种新兴技术，包括云计算、无线传感器、通信技术等，通过健康信息传感器记录、搜集、整合成个人健康档案（PHR, personal health records），并由网络上传至健康信息管理云平台，获得健康服务提供商提供的各种服务。其为个人健康档案的分享提供了便捷的模式，也为更好的个性化健康服务提供了便利。然而，PHR 里包含了大量的个人隐私信息[2]，如既往病史、诊断记录等，这样的分享模式给 PHR 的隐私保护带来了严峻的挑战。

基于属性的加密[3]（ABE, attribute-based encryption）作为一种新的“一对多”加密模式，通过属性来描述用户，在保护数据机密性的同时实现细粒度的访问控制。根据访问策略所处位置的不同，ABE 方案通常可以分为 2 类：密文策略 ABE[4]（CP-ABE, ciphertext-policy ABE）与密钥策略 ABE[5]（KP-ABE, key-policy ABE）。在 CP-ABE 方案中，由数据拥有者利用自定义的访问策略来加密数据，只有用户拥有满足访问策略的属性时才能正确解密，更符合实际需求，从而广泛地应用于 mHealth 系统[6-7]中。

然而，在实际部署 mHealth 系统时，有 2 个问题值得注意。一方面，在单授权机构的方案[3-7]中，该授权机构负责管理整个系统属性域以及所有用户密钥的生成，极易成为系统的性能与安全瓶颈。Chase[8]提出了多授权机构的概念并给出了一种密钥策略 ABE 方案。基于多授权机构方案[9]，Li 等[10]提出了一种云计算中的 PHR 安全分享方案，然而，上述方案[8-10]都是在选择安全模型下证明的，即攻击者需要事先声明要挑战的访问策略或属性集合。Lewko 等[11]提出了适应性安全的多授权机构 CP-ABE 方案，该方案在随机预言机模型下证明。随后，Liu 等[12]提出了标准模型下适应性安全的方案；Li 等[13]提出了针对云存储服务的多授权机构 CP-ABE 方案，与文献[12]的方案相比，该方案只采用一个中央授权机构（CA, central authority），而且该 CA 并不能解密任何密文。

另一方面，系统中某些恶意用户可能出售自己的密钥（白盒）给非法用户以获取不法利益，而在属性加密体系中，属性可以由多个用户共同拥有，因此，很难判断出属性密钥来自哪个用户，这给恶意用户追踪带来了很大困难。针对该问题，Liu 等[14]提出了一种单授权机构下白盒可追踪的 CP-ABE 方案；Li 等[15]提出了一种基于与门策略的可追踪多授权机构 ABE 方案，访问策略较为简单；Guan 等[16]提出了一种移动云计算环境下可追踪 CP-ABE 方案，该方案将授权机构分成 3 个部分，各自执行不同的密钥生成操作。

然而，目前的基于属性的访问控制方案要么致力于支持多个授权机构，要么只在单授权机构情形下考虑恶意用户追踪问题。文献[8-13]的方案考虑多个授权机构并存的问题，但没有考虑恶意用户追踪的问题；文献[14]的方案只在单个授权机构的前提下实现了恶意用户追踪；文献[15-16]的方案安全性是在选择安全模型下证明的。因此，如何构造一种自适应安全的可追踪多授权机构访问控制方案还是一个值得考虑的问题。

本文基于文献[13]的方案，结合追踪技术[14]提出了一种面向 mHealth 的支持多个授权机构的可追踪 CP-ABE 方案，并基于子群判定问题在标准模型下证明其是适应性安全的。方案中包含一个 CA 与多个属性授权机构（AA, attribute authority），AA 负责管理不同的属性域，且不需要通过交互来设置系统参数。为了在多 AA 并存的情形下实现恶意用户追踪，CA 负责生成类似文献[14]方案中的身份追踪参数，但是不会直接参与任何属性相关的操作。AA 基于 CA 生成的身份追踪参数来生成用户密钥，使该密钥可追踪。该方案在合数阶群上构造，支持任意单调的基于线性秘密分享机制（LSSS, linear secret sharing scheme）的访问策略，基于 k-SDH 问题，证明了该方案的可追踪性，性能分析表明了方案的可用性。

2 背景知识

2.1 双线性配对

本文使用了合数阶群上的双线性配对[17],其定义如下。

选取 $\mathbb{G}$ 和 $\mathbb{G}_1$ 为 2 个阶为 $N=p_1p_2p_3$ 的群，其中，p_1、p_2、p_3 是 3 个不同的素数，定义一个可有效计算的双线性映射 $e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_1$，该映射满足以下条件。

1) 双线性：对于所有的 $a,b\in\mathbb{Z}_N$ 和所有的 $u,v\in\mathbb{G}$，有 $e\left(u^a,v^b\right)=e(u,v)^{ab}$。

2) 非退化性：$\exists g\in\mathbb{G}$，使 $e(g,g)$ 在 $\mathbb{G}_1$ 中的阶为 N。

令 $\mathbb{G}_{p_i}$ 表示 $\mathbb{G}$ 的一个阶为 p_i 的子群。注意：对于任意的 $h_i \in \mathbb{G}_{p_i}$ 与 $h_j \in \mathbb{G}_{p_j}$，如果 $i \neq j$，有 $e(h_i, h_j) = 1$。对于 $\mathbb{G}$ 中的元素 T，T 可以写作 $\mathbb{G}_{p_1}$ 中的一个元素、$\mathbb{G}_{p_2}$ 中的一个元素和 $\mathbb{G}_{p_3}$ 中的一个元素的乘积形式。这 3 个元素分别代表 T 的 $\mathbb{G}_{p_1}$、$\mathbb{G}_{p_2}$ 和 $\mathbb{G}_{p_3}$ 部分。

2.2　困难性假设

假设 1[17]　给定一个群生成器 $\mathcal{G}$，定义如下分布。

$$G = (N = p_1 p_2 p_3, \mathbb{G}, \mathbb{G}_1, e) \xleftarrow{R} \mathcal{G}$$

$$g \xleftarrow{R} \mathbb{G}_{p_1}, X_3 \xleftarrow{R} \mathbb{G}_{p_3}$$

$$D = (G, g, X_3)$$

$$T_1 \xleftarrow{R} \mathbb{G}_{p_1 p_2}, T_2 \xleftarrow{R} \mathbb{G}_{p_1}$$

算法 $\mathcal{A}$ 攻破假设 1 的优势定义为 $Adv1_{\mathcal{G},\mathcal{A}} = |\Pr[\mathcal{A}(D, T_1) = 1] - \Pr[\mathcal{A}(D, T_2) = 1]|$。

定义 1　$\mathcal{G}$ 满足假设 1，如果对于任意的多项式时间算法 $\mathcal{A}$，优势 $Adv1_{\mathcal{G},\mathcal{A}}$ 是可忽略的。

假设 2[17]　给定一个群生成器 $\mathcal{G}$，定义如下分布。

$$G = (N = p_1 p_2 p_3, \mathbb{G}, \mathbb{G}_1, e) \xleftarrow{R} \mathcal{G}$$

$$g, X_1 \xleftarrow{R} \mathbb{G}_{p_1}, X_2, Y_2 \xleftarrow{R} \mathbb{G}_{p_2}, X_3, Y_3 \xleftarrow{R} \mathbb{G}_{p_3}$$

$$D = (G, g, X_1 X_2, X_3, Y_2 Y_3)$$

$$T_1 \xleftarrow{R} \mathbb{G}, T_2 \xleftarrow{R} \mathbb{G}_{p_1 p_3}$$

算法 $\mathcal{A}$ 攻破假设 2 的优势定义为 $Adv2_{\mathcal{G},\mathcal{A}} = |\Pr[\mathcal{A}(D, T_1) = 1] - \Pr[\mathcal{A}(D, T_2) = 1]|$。

定义 2　$\mathcal{G}$ 满足假设 2，如果对于任意的多项式时间算法 $\mathcal{A}$，优势 $Adv2_{\mathcal{G},\mathcal{A}}$ 是可忽略的。

假设 3[17]　给定一个群生成器 $\mathcal{G}$，定义如下分布。

$$G = (N = p_1 p_2 p_3, \mathbb{G}, \mathbb{G}_1, e) \xleftarrow{R} \mathcal{G}, \alpha, s \xleftarrow{R} \mathbb{Z}_N$$

$$g \xleftarrow{R} \mathbb{G}_{p_1}, X_2, Y_2, Z_2 \xleftarrow{R} \mathbb{G}_{p_2}, X_3 \xleftarrow{R} \mathbb{G}_{p_3}$$

$$D = (G, g, g^{\alpha} X_2, X_3, g^{s} Y_2, Z_2)$$

$$T_1 = e(g, g)^{\alpha s}, T_2 \xleftarrow{R} \mathbb{G}_1$$

算法 $\mathcal{A}$ 攻破假设 3 的优势定义为 $Adv3_{\mathcal{G},\mathcal{A}} = |\Pr[\mathcal{A}(D, T_1) = 1] - \Pr[\mathcal{A}(D, T_2) = 1]|$。

定义 3　$\mathcal{G}$ 满足假设 3，如果对于任意的多项式时间算法 $\mathcal{A}$，优势 $Adv3_{\mathcal{G},\mathcal{A}}$ 是可忽略的。

2.3　线性秘密共享体制(LSSS)

定义 4[18]　令 $\mathbb{P} = \{P_1, P_2, \cdots, P_T\}$ 表示参与方的集合，$\mathbb{P}$ 上的一个秘密共享方案 Π 被称作线性的，如果：1) 每个参与方关于秘密 s 的份额是 $\mathbb{Z}_N$ 上的一个向量，2) 存在 Π 的一个 l 行 n 列的共享生成矩阵 $\boldsymbol{A}$，令 ρ 为一个从 $\{1,2,\cdots,l\}$ 到 $\mathbb{P}$ 的映射，即 ρ 将矩阵 $\boldsymbol{A}$ 的每一行映射到一个参与方，选择一个随机向量 $\boldsymbol{v} = (s, v_2, \cdots, v_n)^{\mathrm{T}} \in \mathbb{Z}_N^n$，则 $\boldsymbol{Av}$ 是 s 关于 Π 的 l 个共享份额，而且第 i 个份额 λ_i 属于参与方 $\rho(i)$。

文献[18]表明，单调的访问结构与线性秘密共享方案是等价的，且任何一个线性秘密共享方案都具有线性重构的性质。令 $(\boldsymbol{A}, \rho)$ 表示一个访问结构 $\mathbb{A}$，S 为一个授权集合，令集合 $I = \{i : \rho(i) \in S\}$，存在常数 $\{\omega_i \in \mathbb{Z}_p\}_{i \in I}$ 使 $\sum_{i \in I} \omega_i \lambda_i = s$。对于非授权集合，这样的常数是不存在的。本文只考虑每个属性在访问结构中出现一次的情况。

2.4　*k*-SDH 假设（*k*-strong Diffie-Hellman assumption）

令 $\mathbb{G}$ 为一个阶为素数 p 的群，令 g 为群 $\mathbb{G}$ 的一个生成元。*k*-SDH 问题定义如下：随机选择 $k+1$ 元组 $(g, g^x, g^{x^2}, \cdots, g^{x^k})$ 作为输入，输出 $(c, g^{\frac{1}{x+c}}) \in \mathbb{Z}_p \times \mathbb{G}$，一个算法 $\mathcal{A}$ 能够以 ϵ 的优势攻破 *k*-SDH 假设，即

概率 $\Pr[\mathcal{A}(g, g^x, g^{x^2}, \cdots, g^{x^k}) = (c, g^{\frac{1}{x+c}})] \geqslant \epsilon$

定义 5　若没用到至少 ϵ 的优势多项式时间的算法解决 *k*-SDH 问题，则 *k*-SDH 假设成立。

3　系统描述、系统模型和安全模型

3.1　系统描述

系统由 5 个参与方组成：中央授权机构、属性授权机构、PHR 拥有者、mHealth 云、PHR 用户，如图 1 所示。

中央授权机构（CA）：为 PHR 用户生成身份私钥，但是不参与任何属性相关操作。该身份私钥将来自各个属性授权机构的密钥“绑定”起来抵御共谋攻击。

属性授权机构（AA）：生成系统属性相关公开参数，为 PHR 用户生成属性密钥。

PHR 拥有者：其负责生成并整合 PHR 数据，设置访问策略并加密 PHR 上传至 mHealth 云。必要时可以要求 mHealth 云删除其数据。

mHealth 云：负责存储 PHR 拥有者上传的密文数据，本文假设其是诚实但好奇的，即它将诚实地运行系统设置的功能，但是试图去获取加密 PHR 中的隐私信息。

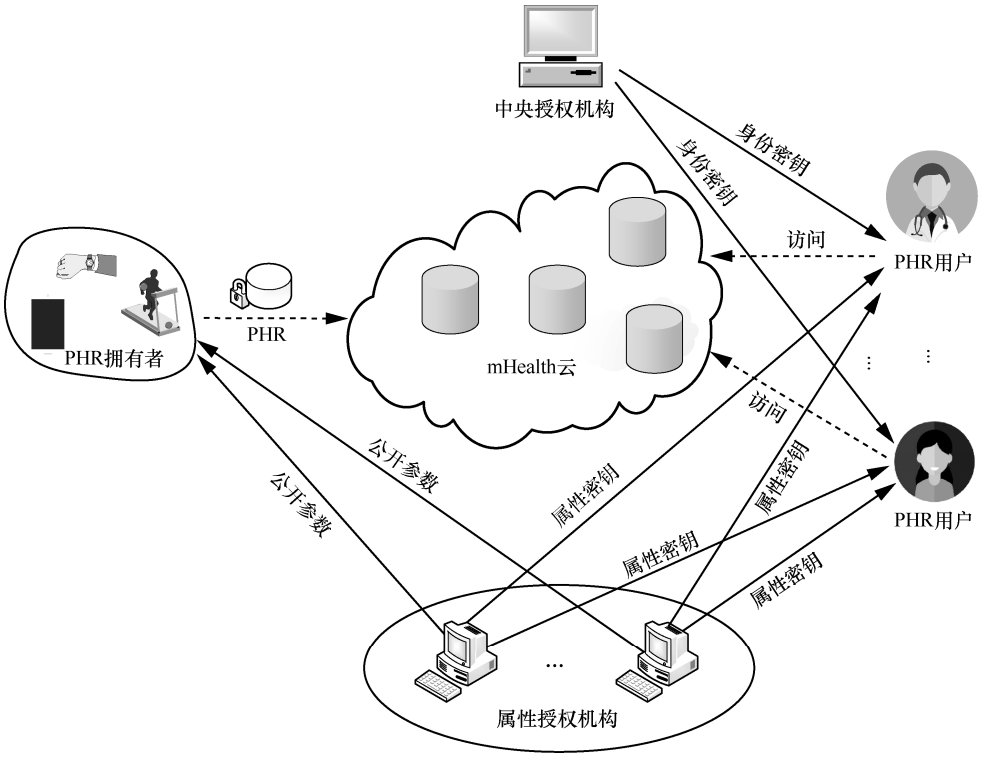

图 1　mHealth 系统框架

PHR 用户：PHR 用户可以利用其密钥来访问加密的 PHR 数据并为其拥有者提供相关医疗服务，但是只有其属性集合满足访问策略的 PHR 用户才能恢复密文，其中某些恶意 PHR 用户可能出售其密钥给非法用户来牟利。

3.2　系统模型

一个可追踪多授权机构 CP-ABE 方案由如下 8 个多项式时间算法组成。

Global Setup $(\lambda)\rightarrow(GPK)$：输入安全参数 λ，输出系统全局参数 GPK。

CA Setup $(GPK)\rightarrow(CPK,CMK)$：输入系统全局参数 GPK、输出中央授权机构 CA 的公开参数 CPK 和主密钥 CMK。此外，初始化身份列表 $IT=\varnothing$。

AA_f Setup $(GPK,f,U_f)\rightarrow(APK_f,AMK_f)$：输入 GPK，授权机构标识 f 及其管理的属性域 U_f，输出属性授权机构 AA_f 的公开参数 APK_f 和其主密钥 AMK_f。

Encrypt $(M,\mathbb{A},GPK,\cup APK_f)\rightarrow(CT)$：输入要加密的消息 M、访问策略 $\mathbb{A}$ 与公开参数 CPK 和相关 AA 的公开参数 $\cup APK_f$，输出密文 CT。

CAKeyGen $(GPK,gid)\rightarrow(IDSK_{gid},CASK_{gid},CAPK_{gid})$：输入 GPK 与用户的全局标识符（gid），输出用户的追踪密钥参数 $IDSK_{gid}$、CA 密钥部分 $CASK_{gid}$ 与 AA 将会用到 $CAPK_{gid}$，并将 gid 和 $IDSK_{gid}$ 记入身份列表 IT。

AA_f KeyGen $(S_{gid,f},GPK,CPK,CAPK_{gid},AMK_f)\rightarrow(ASK_{S,gid,f})$：输入用户的属性集合 $S_{gid,f}$、GPK、CPK、$CAPK_{gid}$ 以及 AMK_f，输出用户属性密钥 $ASK_{S,gid,f}$。

Decrypt $(CT,GPK,CASK_{gid},ASK_{S,gid})\rightarrow(M/\perp)$：输入密文 CT、GPK、$CASK_{gid}$ 以及 $ASK_{S,gid}$，若属性集合 $\cup S_{gid,f}$ 满足访问策略，则输出 M，否则，输出 $\perp$。

Trace $(IT,GPK,\cup APK_f,CASK_{gid},IDSK_{gid},ASK_{S,gid})\rightarrow(gid,\top)$：输入身份列表 IT、GPK、$\cup APK_f$、$CASK_{gid}$、$IDSK_{gid}$ 和 $ASK_{S,gid}$，首先验证 $CASK_{gid}$ 和 $ASK_{S,gid}$ 是否 well-formed，若是，则输出相关 gid。否则，输出 $\top$。well-formed 意味着其可以通过 Key Sanity Check 来确保其可以正常用来解密[14]。

3.3　安全模型

本文通过攻击者 $\mathcal{A}$ 与挑战者 $\mathcal{B}$ 之间的攻击游戏来定义可追踪多授权机构 CP-ABE 方案的安

全模型。

初始化　挑战者 $\mathcal{B}$ 运行方案的 Global Setup、CA Setup 和 AA_f Setup 算法，并将系统的公钥参数发送至攻击者 $\mathcal{A}$。

阶段 1　$\mathcal{A}$ 询问任意的用户属性集合 $(gid_1,S_1),(gid_2,S_2),\cdots,(gid_q,S_q)$，挑战者 $\mathcal{B}$ 返回相对应的密钥。

挑战　$\mathcal{A}$ 提交 2 条长度相等的明文 M_0、M_1 及一个挑战访问策略集合 $\mathbb{A}^*$。$\mathcal{B}$ 从中随机选择一条明文 M_b 用 $\mathbb{A}^*$ 加密，并将挑战密文 CT^* 返回给 $\mathcal{A}$。注意：$\mathbb{A}^*$ 不能是匹配阶段 1 中属性集合的访问策略。

阶段 2　与阶段 1 类似，$\mathcal{A}$ 可以询问密钥，但是 $\mathcal{A}$ 不能查询满足 $\mathbb{A}^*$ 的属性集合。

猜测　$\mathcal{A}$ 输出对 b 的猜测 b'。若 $b'=b$，则 $\mathcal{A}$ 获胜。$\mathcal{A}$ 的优势定义为 $\left|\Pr[b=b']-\frac{1}{2}\right|$。

定义 6　一种可追踪多授权机构 CP-ABE 方案是安全的，当且仅当在上述的攻击游戏中，任何多项式时间攻击者 $\mathcal{A}$ 的优势是可以忽略的。

3.4　可追踪性模型

本节给出本文方案的可追踪性定义，其也是通过挑战者和攻击者之间的交互式游戏来描述的。

初始化　挑战者运行系统 Global Setup、CA Setup 和 AA_f Setup 算法，生成系统公共参数和主密钥，并将公开参数发送给攻击者。

密钥查询　攻击者可以自适应地提交属性集合 $(gid_1,S_1),(gid_2,S_2),\cdots,(gid_q,S_q)$ 进行密钥查询。

密钥伪造　攻击者输出密钥 $SK_\star$，攻击者赢得游戏，若 $Trace(IT,PK,SK)\neq\top$（即该密钥是 well-formed）且 $Trace(IT,PK,SK)\notin\{gid_1,gid_2,\cdots,gid_q\}$，攻击者赢得游戏的概率定义为 $\Pr[Trace(IT,PK,SK)\neq\{\top\}\cup\{gid_1,gid_2,\cdots,gid\}]$。

定义 7　如果对于任意的多项式时间算法而言，一个可追踪的多授权机构 CP-ABE 方案是完全可追踪的，其在上述游戏的优势都是可以忽略的。

4　具体方案

本系统主要由 5 个步骤组成：系统初始化、PHR 上传、用户注册及密钥生成、PHR 访问和恶意用户追踪。

4.1　系统初始化

系统初始化包含 3 种算法：Global Setup、CA Setup 和 AA_f Setup。

Global Setup。令 $\mathbb{G}$ 与 $\mathbb{G}_1$ 为 2 个阶为 N 的群，其中，N 为 3 个不同的素数 p_1、p_2、p_3 的乘积。令 e 是一个 $\mathbb{G}\times\mathbb{G}\to\mathbb{G}_1$ 的双线性映射。从 $\mathbb{Z}_N$ 中选择一个随机数 a，从 $\mathbb{G}_{p_1}$ 中随机选择一个元素 g，计算 g^a。从 $\mathbb{G}_{p_3}$ 中选择一个生成元 X_3。另外，选择一种在适应性选择消息攻击下不可伪造的签名方案 $\sum_{sign}=(KeyGen,Sign,Verify)$。发布全局公钥参数为 $GPK=\left(N,g,g^a,X_3,\sum_{sign}=(KeyGen,Sign,Verify)\right)$，并将 a 发送给属性授权机构。

CA Setup。CA 运行签名算法中的 $KenGen$，输出一对签名密钥 CMK 和验证密钥 CPK。其中，CPK 只会被属性授权机构们使用。同时，置用户列表为 $IT=\varnothing$。

AA_f Setup。每个属性授权机构 AA_f 管理一个属性域 U_f，对于每个属性 $i\in U_f$，从 $\mathbb{Z}_N$ 中选择一个随机数 $t_{f,i}$，并计算 $T_i=g^{t_{f,i}}$，另外，随机选择 $\alpha_f,a_f\in\mathbb{Z}_N$。发布属性授权机构的公开参数 $APK_f=(g^{a_f},e(g,g)^{\alpha_f},T_{f,i}\forall i)$。主密钥 AMK_f 为 $AMK_f=(\alpha_f,a_f,t_{f,i}\forall i)$。

最后，系统公开参数 $PK=(GPK,CPK,\bigcup_{f=1}^{F}APK_f)$，其中，$F$ 表示系统中属性授权机构的数量。

4.2　PHR 上传

对于每个 PHR 文件，PHR 拥有者首先选择一个对称密钥 K 对其加密，密文为 EN_{PHR}，再定义一个 LSSS 访问策略对 K 加密，具体算法如下。

Encrypt。LSSS 访问策略为 $\mathbb{A}(\boldsymbol{W},\rho)$，其中，$\boldsymbol{W}$ 为一个 ℓ 行 n 列的矩阵，ρ 将矩阵的每一行 W_x 映射为属性 $\rho(x)$。随机选择一个列向量 $\boldsymbol{\upsilon}=(s,\upsilon_2,\cdots,\upsilon_n)^{\mathrm{T}}\in\mathbb{Z}_N^n$，对于每一个 $x\in[\ell]$，随机选择一个 $r_x\in\mathbb{Z}_N$，计算 $C=K(\prod_{f\in\mathbb{F}_E}e(g,g)^{\alpha_f})^s$，$C_0=g^s$，$C_1=g^{as}$，$C_x=g^{\sum_{f\in\mathbb{F}_E}a_fW_x\vec{\upsilon}}\cdot T_{\rho(x)}^{-r_x}$，$D_x=g^{r_x}$。其中，$\mathbb{F}_E$ 表示与 W 中属性有关的属性授权机构的集合。

密文 $CT=(\mathbb{A},C,C_0,C_1,\{C_x,D_x\}_{x\in[\ell]})$。收到 CT 与加密的 PHR 文件后，mHealth 云服务提供商为文件定义一个 ID 并以表 1 的形式存在于云端。

表 1　　加密的 PHR 存储形式

标号	属性密文	PHR 密文
ID	CT	EN_{PHR}

4.3　用户注册及密钥生成

当一个 PHR 用户加入系统时，由系统分配给其一个全局身份标识符（gid），利用 CA KeyGen 和 AA_f KeyGen 算法为其生成身份相关及属性相关的密钥，并将其 gid 和身份相关密钥记录入身份列表。

CAKeygen。选择 $c_{gid},t_{gid}\in\mathbb{Z}_N$，$R_{gid},R'_{gid}\in\mathbb{G}_{p_3}$，令 $IDSK_{gid}=c_{gid}$。计算 $CASK_{gid}=(L_{gid},\ L'_{gid})=(g^{t_{gid}}R_{gid},\ g^{at_{gid}}R'_{gid})$，并用 CMK 对元组 $(CMK,gid\|c_{gid}\|CASK_{gid})$ 签名，得到 σ_{gid}，令 $CAPK_{gid}=(gid,c_{gid},CASK_{gid},\sigma_{gid})$，发送 DSK_{gid}、$CAPK_{gid}$ 以及 $CASK_{gid}$ 给用户。同时将 (gid,c_{gid}) 记入用户身份列表 IT。

AA_f Keygen。PHR 用户将 $CAPK_{gid}$ 发送给 AA_f 请求属性集合 $S_{gid,f}$ 的密钥，AA_f 首先利用 CPK 验证签名是否有效，无效则终止；否则，随机选择 $R_{gid,f,0}\in\mathbb{G}_{p_3}$，计算 $K_{gid,f}=g^{\frac{\alpha_f}{a+c_{gid}}}L_{gid}^{a_f}R_{gid,f,0}=g^{\frac{\alpha_f}{a+c_{gid}}}g^{a_f t_{gid}}R_{gid,f}$。对于 $i\in S_{gid,f}$，随机选择 $R'_{gid,f,i}\in\mathbb{G}_{p_3}$，计算 $K_{gid,f,i}=L_{gid}^{(a+c_{gid})t_{fi}}R'_{gid,f,i}=T_{f,i}^{t_{gid}(a+c_{gid})}\cdot R_{gid,f,i}$。本文记 $R_{gid,f}=R_{gid,f,0}R_{gid}^{a_f}$，$R_{gid,f,i}=R_{gid}^{(a+c_{gid})t_{f,i}}\cdot R'_{gid,f,i}$。最后发送 $ASK_{S,gid,f}=(K_{gid,f},\ \{K_{gid,f,i}\}_{i\in S_{gid,f}})$ 给 PHR 用户。

4.4　PHR 访问

PHR 用户可以请求访问 PHR 数据，但是只有那些属性满足 PHR 密文中访问策略的用户才可以正确解密。

Decrypt。若用户的属性集合 $\cup S_{gid,f}$ 满足访问策略 $\mathbb{A}(W,\rho)$，则存在 $\omega_x\in\mathbb{Z}_N$，使 $\sum_{\rho(x)\in S_{gid}}\omega_x W_x=(1,0,\cdots,0)$。计算

$$DEKEY=\frac{e(\prod_{f\in\mathbb{F}_E}K_{gid,f},C_0^{c_{gid}}C_1)}{\prod_{\rho(x)\in S_{gid}}(e(C_x,L_{gid}^{c_{gid}}L'_{gid})e(D_x,K_{\rho(x)}))^{\omega_x}}$$

$$=\frac{e(\prod_{f\in\mathbb{F}_E}g^{\frac{\alpha_f}{a+c_{gid}}}g^{a_f t_{gid}}R_{gid,f},g^{c_{gid}s}g^{as})}{\prod_{\rho(x)\in S_{gid}}(e(g^{\sum_{f\in\mathbb{F}_E}a_f\cdot W_x\vec{v}}T_{\rho(x)}^{-r_x},g^{t_{gid}c_{gid}}g^{at_{gid}})e(g^{r_x},T_{f,i}^{(a+c_{gid})t_{gid}}))^{\omega_x}}$$

$$=e(g,g)^{\sum_{f\in\mathbb{F}_E}\alpha_f s}$$

最后，计算 $K=\dfrac{C}{DEKEY}$。

4.5　恶意用户追踪

如果 SK 是以下形式的：$\cup ASK_{S,gid,f}=\{K_{gid,f},\{K_{gid,f,i}\}_{i\in S_{gid,f}}\},IDSK_{gid},L'_{gid},L_{gid}$，并且满足以下 Key Sanity Check 的 4 个验证步骤，则它表示属性集合 $S_C=\{x\,|\,x\in\mathrm{S}_{gid}\wedge e(\mathrm{T}_{f,i},L_{gid}^{c_{gid}}L'_{gid})=e(g,K_{gid,f,i})\neq 1\}$ 对应的访问权限，否则输出 ⊤。如果 SK 是 well-formed，则算法在 IT 中搜索 c_{gid}，若能搜索到，则输出其全局身份标识符 gid，否则输出一个从未出现过的身份 $gid*$。

Key Sanity Check

1) $IDSK_{gid}\in\mathbb{Z}_N$，$K_{gid,f},K_{gid,f,i},L'_{gid},L_{gid}\in\mathbb{G}$

2) $e(g,L'_{gid})=e(g^a,L_{gid})\neq 1$

3) $e(g^a g^{c_{gid}},K_{gid,f})=e(g,g)^{\alpha_f}e(g^{a_f},L_{gid}{}^{c_{gid}}L'_{gid})\neq 1$

4) $\exists i\in S_C$，s.t. $e(T_{f,i},\ L_{gid}{}^{c_{gid}}L'_{gid})=e(g,K_{gid,f,i})\neq 1$

5　安全性证明与可追踪性证明

5.1　安全性证明

与文献[14]的方案类似，本文方案的安全性规约至文献[13] 的方案安全性，为了简便，本文将文献[13]的方案表示为 $\sum_{\text{MCP-ABE}}$，本文方案表示为 $\sum_{\text{T-MCP-ABE}}$。

引理 1[13]　若子群判断假设 1~假设 3 成立，则方案 $\sum_{\text{MCP-ABE}}$ 在标准模型下是适应性安全的。

具体的证明可以参考文献[13]的方案。

下面，给出方案 $\sum_{\text{T-MCP-ABE}}$ 的安全性证明。

引理 2　若方案$\sum_{\text{MCP-ABE}}$是安全的，则本文方案$\sum_{\text{T-MCP-ABE}}$在第 3.3 节给出的安全模型下也是安全的。

证明　假设存在一个多项式时间攻击者$\mathcal{A}$以优势$ADV_{\mathcal{A}}\sum_{\text{T-MCP-ABE}}$攻破本文方案，则本文可以构造一个多项式时间挑战者$\mathcal{B}$以相等的优势$ADV_{\mathcal{B}}\sum_{\text{MCP-ABE}}$攻破方案$\sum_{\text{MCP-ABE}}$。

初始化　$\sum_{\text{MCP-ABE}}$发送公开参数$PK_{\text{MCP-ABE}}=(GPK,CPK,\bigcup_{f=1}^{F}APK_f)$给$\mathcal{B}$。$\mathcal{B}$从$\mathbb{Z}_N$中选择一个随机数$a$，计算$g^a$。然后发送$PK_{\text{T-MCP-ABE}}=(g^a,GPK,CPK,\bigcup_{f=1}^{F}APK_f)$给攻击者$\mathcal{A}$。

阶段 1　当$\mathcal{A}$提交属性集合(gid,S)来请求私钥时，$\mathcal{B}$发送(gid,S)至$\sum_{\text{MCP-ABE}}$得到密钥$DSK_{gid}=c_{\text{M-}gid}$，$CASK_{\text{M-}gid}=L_{\text{M-}gid}=g^{\frac{t_{\text{M-}gid}}{c_{\text{M-}gid}}}R_{\text{M-}gid}$，$\bigcup ASK_{S,\text{M-}gid,f}=\bigcup\{(K_{\text{M-}gid,f},\{K_{\text{M-}gid,f,i}\}_{i\in S_{\text{M-}gid,f}})\}$。其中，$K_{\text{M-}gid,f}=g^{\frac{\alpha_f}{c_{\text{M-}gid}}}g^{\frac{a_f t_{\text{M-}gid}}{c_{\text{M-}gid}}}R_{gid,f}$，$K_{\text{M-}gid,f,i}=T_{f,i}^{\frac{t_{\text{M-}gid}}{c_{\text{M-}gid}}}R_{gid,f,i}$。值得注意的是，方案$\sum_{\text{MCP-ABE}}$的密钥中设置$DSK_{gid}$主要是用来实现外包解密功能的。

得到密钥以后，$\mathcal{B}$做如下处理，随机选择$c_{gid}\in\mathbb{Z}_N^*$，并计算$\frac{1}{a+c_{gid}}\bmod N$，若$gcd(a+c_{gid},N)\neq 1$或$c_{gid}$已经存在于用户身份列表$IT$中，则重新选择$c_{gid}$。令$t_{gid}=\frac{t_{\text{M-}gid}}{a+c_{gid}}$，计算$CASK_{gid}=(CASK_{\text{M-}gid})^{\frac{c_{\text{M-}gid}}{a+c_{gid}}}=L_{gid}=g^{t_{gid}}R_{gid}$，$L_{gid}^{'}=(CASK_{\text{M-}gid})^{\frac{ac_{\text{M-}gid}}{a+c_{gid}}}=g^{at_{gid}}R_{gid}^{'}$，$K_{gid,f}=(K_{\text{M-}gid,f})^{\frac{c_{\text{M-}gid}}{a+c_{gid}}}=g^{\frac{\alpha_f}{a+c_{gid}}}g^{a_f t_{gid}}R_{gid,f}$，$K_{gid,f,i}=(K_{\text{M-}gid,f,i})^{c_{\text{M-}gid}}=T_{f,i}^{t_{gid}(a+c_{gid})}R_{gid,f,i}$，$CAPK_{gid}$也可以类似得到。

最后，$\mathcal{B}$将c_{gid}、$CAPK_{gid}$、$CASK_{gid}$、$L_{gid}^{'}$以及$\bigcup ASK_{S,gid,f}=\bigcup\{(K_{gid,f},\{K_{gid,f,i}\}_{i\in S_{gid,f}})\}$发送给$\mathcal{A}$。同时将$(gid,c_{gid})$记入用户身份列表$IT$。

挑战　$\mathcal{A}$提交 2 个等长的消息M_0、M_1以及访问策略$\mathbb{A}(W,\rho)$，$\mathcal{B}$将其发送至$\sum_{\text{MCP-ABE}}$，$\sum_{\text{MCP-ABE}}$返回密文$C_{\text{MCP-ABE}}=M(\prod_{f\in\mathbb{F}_E}e(g,g)^{\alpha_f})^s$，$C_{0\text{-MCP-ABE}}=g^s$，$C_{x\text{-MCP-ABE}}=g^{\sum_{f\in\mathbb{F}_E}a_f W_x\vec{v}}T_{\rho(x)}^{-r_x}$，$D_{x\text{-MCP-ABE}}=g^{r_x}$。$\mathcal{B}$除了计算$C_1=(C_{0\text{-MCP-ABE}})^a=g^{as}$之外，别的密文组件都不做变动。最后，将$CT=(\mathbb{A},C,C_0,C_1,\{C_x,D_x\}_{x\in[\ell]})$发送给$\mathcal{A}$。

阶段 2　与阶段 1 类似，但是不能查询满足挑战的访问策略的密钥。

猜测　$\mathcal{A}$返回一个猜测b'给$\mathcal{B}$，$\mathcal{B}$将其返回给$\sum_{\text{MCP-ABE}}$。

注意，公开参数、密钥和密文的分布都与真实方案一样。因此，优势$ADV_{\mathcal{A}}\sum_{\text{T-MCP-ABE}}=ADV_{\mathcal{B}}\sum_{\text{MCP-ABE}}$。

定理 1　若假设 1~假设 3 成立，则本文方案在标准模型下是适应性 CPA 安全的。

证明　由引理 2 可得，若$\sum_{\text{MCP-ABE}}$是 CPA 安全的，则本文方案也是 CPA 安全的。由引理 1 可得，若假设 1~假设 3 成立，则$\sum_{\text{MCP-ABE}}$在标准模型下是适应性 CPA 安全的。

综上所述，定理 1 成立。

5.2　可追踪性证明

与文献[14]的方案类似，本文也基于假设 3 和k-SDH 假设来证明方案的可追踪性。

定理 2　若假设 3 和k-SDH 假设成立，则本文方案$\sum_{\text{T-MCP-ABE}}$在$q<k$情况下是完全可追踪的。

证明　假设多项式时间算法$\mathcal{A}$在询问q次以后能够以不可忽略的优势ϵ赢得可追踪性交互式游戏，不失一般性，令$k=q+1$，则本文可以构造一个仿真者$\mathcal{B}$以不可忽略的优势攻破假设 3 和k-SDH 假设。简便起见，本文只给出$\mathcal{B}$利用k-SDH 问题的参数与$\mathcal{A}$进行可追踪性游戏交互的具体过程。而利用假设 3 给出的参数与$\mathcal{A}$的交互过程可以与文献[14]的方案类似。$\mathcal{B}$以$\mathbb{Z}_N$、$\mathbb{G}$、$\mathbb{G}_1$、e、X_3、$\{A_i=\theta^{a^i}\}_{i=1,\cdots,k}$为输入与$\mathcal{A}$交互的过程如下所示。

Setup。$\mathcal{B}$选择q个不同的随机数$m_1,\cdots m_q\in$

$\mathbb{Z}_N^*$，令多项式 $f(y)=\prod_{i=1}^{q}(y+m_i)$，展开可得 $f(y)=\sum_{i=0}^{q}\eta_i y^i$，其中，$\eta_i\in\mathbb{Z}_N$ 为多项式 $f(y)$ 的系数。$\mathcal{B}$ 计算 $g=\prod_{i=0}^{q}(A_i)^{\eta_i}=\theta^{f(a)}\in\mathbb{G}_{p_1}$，$g^a=\prod_{i=0}^{q+1}(A_i)^{\eta_{i-1}}=\theta^{f(a)\cdot a}$。随机选择 $\alpha_f,a_f\in\mathbb{Z}_N$，类似地，对于每个属性 $i\in U_f$，从 $\mathbb{Z}_N$ 中选择一个随机数 $t_{f,i}$，并计算 $T_i=g^{t_{f,i}}$，

最后，发送 $(GPK,CPK,\bigcup_{f=1}^{F}APK_f)$ 给 $\mathcal{A}$。

密钥查询 假设在第 $j\leqslant q$ 次查询的属性集合是 (gid,S_j)，令 $f_j(y)=\frac{f(y)}{y+m_j}=\prod_{i=1,i\neq j}^{q}(y+m_i)$，展开可得 $f_j(y)=\sum_{i=0}^{q-1}\beta_i y^i$，$\mathcal{B}$ 计算 $\chi_j\leftarrow\prod_{i=0}^{q-1}(A_i)^{\beta_i}=\theta^{f_j(a)}=\theta^{\frac{f(a)}{a+m_j}}=g^{\frac{1}{a+m_j}}$，随机选择 $t_{gid}\in\mathbb{Z}_N$，R_{gid}，$R'_{gid},R_{gid,f},R_{gid,f,i}\in G_{p_3}$，$c_{gid}=m_j$，$L_{gid}=g^{t_{gid}}R_{gid}$，$L'_{gid}=g^{at_{gid}}R'_{gid}$，$K_{gid,f}=(\chi_j)^{\alpha_f}g^{a_f t_{gid}}R_{gid,f}=g^{\frac{\alpha_f}{a+c_{gid}}}g^{a_f t_{gid}}R_{gid,f}$，对于每个属性 i，计算 $K_{gid,f,i}=(g^a g^{c_{gid}})^{t_{gid}t_{f,i}}R_{gid,f,i}=T_{f,i}^{t_{gid}(a+c_{gid})}R_{gid,f,i}$。

最后，发送 c_{gid}、$CAPK_{gid}$、$CASK_{gid}$、L'_{gid} 以及 $\cup ASK_{S,gid,f}=\cup\{(K_{gid,f},\{K_{gid,f,i}\}_{i\in S_{gid,f}})\}$ 给 $\mathcal{A}$。

密钥伪造 $\mathcal{A}$ 返回一个密钥 $SK_\star$ 给 $\mathcal{B}$，根据分析[14]，在上述游戏过程定义的公开参数和密钥都与真实方案的分布无异。令 $\Im_{\mathcal{A}}$ 表示 $\mathcal{A}$ 赢得游戏的事件，即是 well-formed，满足 Key Sanity Check，并且 c_{gid} 从未在身份列表中出现过。若 $\Im_{\mathcal{A}}$ 未发生，则 $\mathcal{B}$ 随机选择 $b'\in\{0,1\}$ 和 $(c_r,w_r)\in\mathbb{Z}_{p_1}\times\mathbb{G}_{p_1}$，并分别将其作为结果返回给假设 3 和 k-SDH 假设。

若 $\Im_{\mathcal{A}}$ 发生，用长除法记 $f(y)=\gamma(y)(y+c_{gid})+\gamma_{-1}$，其中，$\gamma(y)=\sum_{i=0}^{q-1}\gamma_i y^i$，$\gamma_{-1}\in\mathbb{Z}_N$ 且 $\gamma_{-1}\neq 0$。$\mathcal{B}$ 计算 $gcd(\gamma_{-1},N)$。

1) 若 $gcd(\gamma_{-1},N)=1$

若 $\mu=0$，则意味着 $\mathcal{A}$ 无法提供任何有用的信息，则 $\mathcal{B}$ 随机选择 $b'\in\{0,1\}$ 和 $(c_r,w_r)\in\mathbb{Z}_N\times\mathbb{G}_1$，并分别将其作为结果返回给假设 3 和 k-SDH 假设。

若 $\mu=1$，则意味着 $\mathcal{B}$ 可以利用 k-SDH 假设与 $\mathcal{A}$ 交互，$\mathcal{B}$ 随机选择 $b'\in\{0,1\}$ 作为结果返回给假设 3，并计算 $(c_r,w_r)\in\mathbb{Z}_{p_1}\times\mathbb{G}_{p_1}$，结果如下所示。

假设 $L_{gid}=g^{t_{gid}}L_2L_3$，其中，$t_{gid}\in\mathbb{Z}_N$，$L_2\in\mathbb{G}_{p_2}$，$L_3\in\mathbb{G}_{p_3}$ 都是未知的。因为该密钥可以通过 Key Sanity Check，因而本文有 $L'_{gid}=g^{at_{gid}}L_{2,1}L_{3,1}$，$K_{gid,f}=g^{\frac{\alpha_f}{a+c_{gid}}}g^{a_f t_{gid}}K_2K_3$，其中，$L_{2,1},K_2\in\mathbb{G}_{p_2}$，$L_{3,1},K_3\in\mathbb{G}_{p_3}$。

$\mathcal{B}$ 计算：$\frac{1}{\gamma_{-1}}\bmod N$，

$$\xi\leftarrow\left(\left(\frac{K_{gid,f}}{(L_{gid})^{a_f}}\right)^{p_2p_3}\right)^{(p_2p_3\alpha_f)^{-1}\bmod p_1}$$

$$=g^{\frac{1}{a+c_{gid}}}=\theta^{\gamma(y)}\theta^{\frac{\gamma_{-1}}{a+c_{gid}}}$$

$$w_r\leftarrow\left(\xi\prod_{i=0}^{q-1}(A_i)^{-\gamma_i}\right)^{\frac{1}{\gamma_{-1}}}=\theta^{\frac{1}{a+c_{gid}}}\in\mathbb{G}_{p_1}$$

$$c_r\leftarrow c_{gid}\bmod p_1\in\mathbb{Z}_{p_1}$$

由于 $e(\theta^a\theta^{c_r},w_r)=e(\theta,\theta)$，则 (c_r,w_r) 是解决 k-SDH 问题的一个可行结论。

2) 若 $gcd(\gamma_{-1},N)\neq 1$

$\mathcal{B}$ 随机选择 $(c_r,w_r)\in\mathbb{Z}_{p_1}\times\mathbb{G}_{p_1}$，并将其作为结果返回 k-SDH 假设。

综上所述，根据文献[14]的方案分析，$\mathcal{B}$ 以至少 $\frac{\varepsilon}{8}$ 的概率攻破假设 3 或以至少 $\frac{\varepsilon}{8}$ 的概率攻破 k-SDH 假设。

证毕。

6 性能分析

表 2 给出了相关多授权机构方案与可追踪方案的特征比较。从表 2 可以看出，本文提出的方案同时支持多个授权机构、适应性安全以及恶意用户追踪。

本文主要统计初始化、加密、密钥生成解密以及追踪算法中用到指数运算和双线性配对的次数，如表 3 所示。令 $|U|$、$|W|$、$|S|$、$|I|$、$|S_T|$ 分别表示属性域、访问策略、用户属性集合、解密时用到的属性集合以及被追踪属性集合中属性个数。令

表 2　　**相关多授权机构方案与可追踪方案的特征比较**

方案	访问策略	多授权机构	安全模型	可追踪性
文献[6]	与门	否	选择性	是
文献[12]	LSSS	是	适应性	否
文献[13]	LSSS	是	适应性	否
文献[14]	LSSS	否	适应性	是
文献[15]	与门	是	选择性	是
文献[16]	树	否	选择性	是
本文	LSSS	是	适应性	是

表 3　　**相关多授权机构方案与可追踪方案的计算开销**

步骤	文献[13]的计算开销	文献[14] 的计算开销	本文的计算开销
初始化	$(\|U\|+\|F_U\|)E_1+\|F_U\|P$	$(\|U\|+1)E_1+1P$	$(\|U\|+\|F_U\|+1)E_1+\|F_U\|P$
加密	$(3\|W\|+1)E_1+1E_2$	$(3\|W\|+2)E_1+1E_2$	$(3\|W\|+2)E_1+1E_2$
密钥生成	$(2\|F_E\|+\|S\|+2)E_1$	$(\|S\|+4)E_1$	$(2\|F_E\|+\|S\|+2)E_1$
解密	$1E_2$	$2E_1+\|I\|E_2+(2\|I\|+1)P$	$2E_1+\|I\|E_2+(2\|I\|+1)P$
追踪	无	$2E_1+(2\|S_T\|+5)P$	$2E_1+(2\|S_T\|+3\|F_T\|+2)P$

$|F_U|$、$|F_E|$与$|F_T|$分别表示系统中、加密时用到的以及追踪密钥涉及的属性授权机构的个数。令 E_1 和 E_2 分别表示 $\mathbb{G}$ 与 $\mathbb{G}_1$ 群中一次指数运算，令 P 表示一次双线性配对的次数。

从表 3 可以看出，与文献[13]的方案相比，为了实现可追踪性，本文方案在初始化、加密以及密钥生成步骤的开销与文献[13]的方案基本无异，只在初始化和加密步骤多了一次指数运算开销，而密钥生成步骤基本一致。因为文献[13]的方案使用了外包解密技术将绝大部分的解密开销外包至云端，所以用户端的解密开销为常数，本文下一步也将考虑如何在支持可追踪性的前提下降低用户的解密开销。文献[14]的方案与本文方案都支持可追踪性，不同点在于文献[14]的方案仅支持单个的授权机构。本文增加的开销主要与系统中的授权机构相关，与各步骤中涉及的属性个数是无关的。综上所述，本文方案的开销是可以接受的。

本文基于JPBC库[19]选择了一个TYPE A1的椭圆曲线群来作为本文方案的运算基础，其群阶为 3 个 517 bit 素数的乘积。在笔记本电脑（WIN 7，CPU 为 2.4 GHz，内存为 6 GB）上进行了仿真。令$|U|$=100，$|W|=|S|=|I|=|S_T|$=10，$|F_U|=|F_E|=|F_T|$=5。实验结果如表 4 所示，其验证了方案性能与理论分析的一致性。

表 4　　**方案计算开销比较**

步骤	方案的计算开销/s		
	文献[13]	文献[14]	本文
初始化	96.75	90.55	97.64
加密	28.25	29.18	29.14
密钥生成	19.58	12.46	19.56
解密	0.08	16.41	16.40
追踪	无	18.28	26.20

7　结束语

本文给出了一个面向 mHealth 的可追踪多授权机构的访问控制方案，并在标准模型下证明了其适应性安全，多个 AA 各自管理一个独立的属性域，并不需要通过协商来设置公开参数。本文方案支持任意单调的访问控制策略，为了达到适应性安全，本文方案在合数阶群上构造，其开销相比素数阶群上选择安全方案而言，开销较大。本文下一步的工作将以提出的方案为基础，结合可验证的外包解密技术，研究高效的适应性安全可追踪方案。

参考文献：

[1] PANAYIOTOU C, SAMARAS G. A mobile agent approach for ubiquitous and personalized eHealth information systems[J]. Personalisa-

tion for E, 2008:792.
[2] ZHANG K, YANG K, LIANG X, et al. Security and privacy for mobile healthcare networks[J]. IEEE Wireless Communications, 2015, 22(4): 104-112.
[3] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]//Advances in Cryptology EUROCRYPT 2005, Lecture Notes in Computer Science. 2005: 457-473.
[4] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//The 13th ACM conference on Computer and communications security. 2006: 89-98.
[5] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//Symposium on Security and Privacy. 2007: 321-334.
[6] HAHN C, KWON H, HUR J. Efficient attribute-based secure data sharing with hidden policies and traceability in mobile health networks[J]. Mobile Information Systems, 2016: 13.
[7] ALSHEHRI S, RADZISZOWSKI S, AND RAJ R. Secure access for healthcare data in the cloud using ciphertext-policy attribute-based encryption[C]//IEEE 28th International Conference on Data Engineering Workshops (ICDEW '12), 2012: 143-146.
[8] CHASE M. Multi-authority attribute based encryption [M]// Theory of Cryptography. Springer Berlin Heidelberg, 2007: 515-534.
[9] CHASE M, CHOW S S M. Improving privacy and security in multi-authority attribute-based encryption[C]// Conference on Computer and Communications Security. 2009: 121-130.
[10] LI M, YU S, ZHENG Y, et al. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption[J]. IEEE Transactions on Parallel & Distributed Systems, 2012, 24(1): 131-143.
[11] LEWKO A, WATERS B. Decentralizing attribute-based encryption[C]//International Conference on the Theory and Applications of Cryptographic Techniques. 2010:568-588.
[12] LIU Z, CAO Z, HUANG Q, et al. Fully secure multi-authority ciphertext-policy attribute-based encryption without random oracles[C]// European Conference on Research in Computer Security. 2011: 278-297.
[13] LI Q, MA J, LI R, et al. Secure, efficient and revocable multi-authority access control system in cloud storage[J]. Computers & Security, 2016, 59(C):45-59.
[14] LIU Z, CAO Z, WONG D S. White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(1):76-88.
[15] LI J, HUANG Q, CHEN X, et al. Multi-authority ciphertext-policy attribute-based encryption with accountability[C]//The 6th ACM Symposium on Information, Computer and Communications Security. 2011: 386-390.
[16] GUAN Z, LI J, ZHANG Y, et al. An efficient traceable access control scheme with reliable key delegation in mobile cloud computing[J]. EURASIP Journal on Wireless Communications and Networking, 2016, 2016(1): 208.
[17] LEWKO A, OKAMOTO T, SAHAI A, et al. Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption[C]// International Conference on Theory and Applications of Cryptographic Techniques. 2010:62-91.
[18] BEIMEL A. Secure schemes for secret sharing and key distribution[J]. DSc Dissertation, 1996.
[19] CARO A D, IOVINO V. jPBC: Java pairing based cryptography[J]. Proceedings - International Symposium on Computers and Communications, 2011, 22(3):850-855.

[作者简介]

李琦（1989-），男，江苏淮安人，博士，南京邮电大学讲师，主要研究方向为基于属性的密码学与访问控制技术。

朱洪波（1956-），男，江苏扬州人，南京邮电大学教授、博士生导师，主要研究方向为泛在无线通信与物联网技术、宽带无线通信、无线通信与电磁兼容。

熊金波（1981-），男，湖南益阳人，博士，福建师范大学副教授、硕士生导师，主要研究方向为云数据安全、移动数据安全等。

莫若（1990-），男，陕西渭南人，西安电子科技大学博士生，主要研究方向为数字签名。