文章编号:1671-4598(2020)01-0200-05 DOI:10.16526/j.cnki.11—4762/tp.2020.01.042 中图分类号:TP309 文献标识码:A

基于改进 CP—ABE 模型的医疗数据隐私保护管理设计与应用

贾瑞龙[1], 曹亚州[1], 苗俊青[1], 赵 沛[1,2]
(1. 克孜勒苏柯尔克孜自治州人民医院, 新疆 克孜勒苏柯尔克孜 845350;
2. 南京医科大学第一附属医院, 南京 210000)

摘要: 物联网设备监测患者的健康状况, 并将收集到的数据作为电子病历 (EMR) 上传到云端进行存储和共享; 将电子病历外包给云会带来新的安全隐患; 提出了一种新的架构模型, 以确保外包健康记录的安全性; 该模型利用偏序集合 (POSET) 构造基于组的访问结构, 利用基于密文策略的属性加密 (CP—ABE) 提供细粒度的 EMR 访问控制; 改进后的基于 CP—ABE (G—CP—ABE) 的组通过减少访问树中的叶节点数量, 将运算量降至最低; 将对称加密和 CP—ABE 方案合并在一起, 以最大程度地减少总体加密时间; 因此, 即使是资源受限的物联网设备, G—CP—ABE 仍可用于监视健康状况; 性能分析表明了该模型的有效性, 适合于实际应用。

关键词: CP—ABE 模型; 数据隐私; 电子病历; 访问控制

Design and Application of Clinical Data Privacy Protection Management Based on Improved CP—ABE Model

Jia Ruilong[1], Cao Yazhou[1], Miao Junqing[1], Zhao Pei[1,2]
(1. People's Hospital of Kizilsu Kirgiz Autonomous Prefecture, Kizilsu Kirgiz 845350, China;
2. The First Affiliated Hospital of Nanjing Medical University, Nanjing 210000, China)

Abstract: Internet of things devices monitor the health status of patients, and upload the collected data as EMR to the cloud for storage and sharing. Outsourcing electronic medical records to the cloud will bring new security and privacy risks. A new architecture model is proposed to ensure the security and privacy of outsourcing health records. In this model, POSET is used to construct group based access structure, and CP—ABE is used to provide fine—grained EMR access control. The improved group based on g—CP—ABE reduces the number of leaf nodes in the access tree to minimize the computation. The symmetric encryption and CP—ABE scheme are combined to minimize the overall encryption time. Therefore, g—CP—ABE can still be used to monitor the health status of Internet of things devices with limited resources. Performance analysis shows that the model is effective and suitable for practical application.

Keywords: CP—ABE model; data privacy; EMR; access control

0 引言

云计算和物联网的巨大潜力使得互联医疗设备[1-2]和传感器提供高效医疗服务。在医疗保健系统中, 诸多硬件设备 (智能手机、平板电脑、RFID、传感器、植入式医疗设备) 将连接到互联网, 助力于提供信息和服务。相关信息以电子病历形式记录下来, 并上传到云端进行共享[3]。实际上, 当在云中存储或处理数据时, 数据所有者失去了对数据的控制。由于健康记录存储着非常敏感的信息, 因此在云中共享和存储电子病历仍然是一个巨大的隐患。

收稿日期:2019-11-03; **修回日期**:2019-12-05。
基金项目:新疆克州 3123 人才课题(RK2019094)。
作者简介:贾瑞龙(1989-),男,甘肃陇西人,主要从事医疗信息技术与网络管理方向的研究。
通讯作者:赵 沛(1982-),男,江苏徐州人,硕士,副研究员,主要从事医院管理方向的研究。

基于属性的加密 (ABE)[4-6]分为即密钥策略 ABE (KP—ABE) 和密文策略 ABE (CP—ABE), CP—ABE 在 EMR 系统中非常有用。现有的 CP—ABE 方案大多使用双线性映射, 并生成大尺寸的密钥和密文。密钥和密文的大小与所涉及的属性成线性关系, 而双线性对的数量与属性的大小成正比。

本文利用 POSET 创建基于组的访问结构的方法, 减少了加/解密过程中双线性对的数量, 从而大幅减少加/解密运算负担。G—CP—ABE 模型融合了对称加密和 CP—ABE 方案[7-9], 有效地实现了数据的保密性和访问的隐私性。

1 方法论

在 EMR 数据外包的访问策略构建中, 采用 CP—ABE 方案使得外包数据的计算效率成为一个真正的挑战。CP—ABE 加密涉及许多昂贵的双线性对操作, 并且双线性对的数量随属性的数量线性增加。该研究揭示了改进和优化现有解决方案以提高 CP—ABE 性能的机会。目前, 优化技术

广泛存在，并且这些技术在工程应用的各个领域发挥着巨大的作用。现有的工作大多都集中在通过直接采用 CP－ABE 在密文中嵌入访问策略，或者将计算外包给第三方。这两种方法都不适用于大型 EMR 表，因为双线性配对操作的数量与属性的数量和访问树的深度成正比。鉴于这些挑战，提出的安全框架旨在使用基于 POSET 的组访问策略[10-11]来减少双线性配对。此外，EMR 表使用更快的对称加密进行加密，并且访问策略嵌入到密钥密文中，从而显着减少了总体加密和解密时间。

1.1　双线性映射

假设 g 为 G_1 的发生器。通常，G_1 为椭圆曲线，G_2 为有限域。用 e 描述一个双线性映射，$e:G_1 \times G_1 \rightarrow G_2$。双线性映射 e 具有以下属性：

1）双线性：对于 G_1 中所有的 p 和 q 以及 Z_p 中的 a 和 b，有 $e(p^a,q^b)=e(p,q)^{ab}$；

2）非简并性：在 G_1 中存在 p 和 q 使得 $e(p,q)\neq 1$；

3）可计算性：对于 G_1 中所有 p 和 q，均可计算 $e(p,q)$。

双线性映射 e 的计算具有对称性，即 $e(p^a,p^b)=e(p,p)^{ab}=e(p^b,p^a)$。

1.2　访问结构

假设 $\{1,2,\cdots,n\}$ 为一个数组，如果对于任意集合 B，C，有 $B\in A, B\subseteq C, C\in A$，则集合 $A\subseteq 2^{\{1,2\cdots n\}}$ 是单调的。

单调访问结构是由 $2^{\{1,2\cdots n\}}$ 个非空子集组成的集合 A。A 中的集称为授权集，而不是 A 中的集称为未授权集。在本文中，组是属性，访问结构是属性的授权集。

CP－ABE 包含四种基本算法：设置、密钥生成（KeyGen）、加密和解密。令 U 为描述数据属性和用户属性的通用属性集。

1）设置：以隐式安全参数作为输入，生成公钥 PK 和主密钥 MK。

2）密钥生成 $(MK,S)\rightarrow SK_S$：密钥生成将主密钥 MK 和一组属性 S 作为输入，并将与 S 关联的密钥输出到 SK_S。

3）加密 $(PK,M,A)\rightarrow C$：数据所有者执行加密，该算法将输入作为公钥 PK、消息 M 和在 U 上定义的访问结构 A。根据 A 进行加密，并输出密文 CT（假设密文包含访问结构 A）。

4）解密 $(PK,C,SK_S)\rightarrow M$：数据用户运行解密算法，解密算法将公钥 PK、密文 C 和用户密钥 SK_S 作为输入。如果 SK_S 满足访问结构 A，则输出原始消息 M。

1.3　CP－ABE 的安全模型

运行设置算法并向对手交付公钥 PK。

阶段 1：对手对一组属性 $S_1,S_2,\cdots,S_{q1}$ 进行重复密匙操作。

对手提交两条消息 M_1 和 M_2，其中 $|M_1|=|M_2|$。同样，对手提交的质询访问结构为 A^*，其中阶段 1 中的所有 S_i 都不满足 A^*，挑战者猜测一个随机的 b 位，并使用一个 CT^* 向对手加密 M_b。

阶段 2：以 S_i 不满足 A^* 的限制重复阶段 1。

对手输出 b 的猜测位为 $b'\in\{0,1\}$，若 $b'=b$，则对手获胜。

CP－ABE 的安全模型可以很容易地扩展，以管理选定的密文攻击。

2　改进 G－CP－ABE 模型

隐私感知安全框架 Group CP－ABE（G－CP－ABE）被用于管理外包给云的 EMR 的访问控制。该架构使医疗系统能够处理物联网设备产生的海量数据，以实现对病人的监护与管理。由于所收集的数据是非常敏感和私人的健康信息，因此该模型可确保数据的机密性和访问的隐私性。图 1 显示了系统中的主要实体。

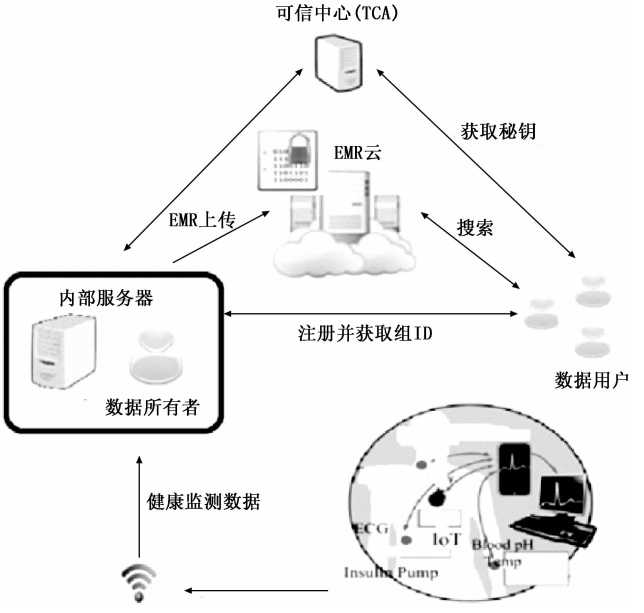

图 1　G－CP－ABE 体系结构

可信中心（TCA）：根据真实的属性集，使用唯一的组密钥初始化每个组。

EMR 数据所有者：为每个组定义访问结构，并在执行加密之前上载到 EMR 云。

EMR 云：云服务提供商被视为半可信实体，它提供存储和其他数据交易服务。

数据用户：数据用户想要访问云中的 EMR，可以从云中下载 EMR，并根据满意的组访问结构进行解密。

物联网设备（传感器、心电监护仪、呼吸监视器及其他等植入式医疗设备）持续监测患者的健康状况，并将这些信息发送到服务器。内部服务器聚合、处理，并将这些数据作为 EMR 上传。

数据所有者可以创建和管理少量组，因为对于任何医疗保健系统，系统的用户都可以很轻松地预定。假设该体系结构遵循集中式组管理。用 $(C,\leqslant)$ 表示层次结构组组织，其中 $\leqslant$ 为 C 上的偏序。显然 $(C,\leqslant)$ 是一个偏序集（POSET）。组表示用户集合，任何两个组都是不相交的。任何一个偏序集都可以表示为一个访问图 $G=(V,E)$，其中

顶点表示组，边表示从上一个到下一个的连接性。G 为一个有向无环图。下面给出组访问结构的详细信息。

2.1 组访问策略

如表 1 中的 EMR 表所示，表中有五个字段，基于“与”门创建的访问结构如图 2 所示。

表 1 医院中的 EMR

ID(A)	姓名(B)	年龄(C)	疾病名称(D)	症状(E)
A00125	张三	38	水痘	发烧
A01345	李四	21	风湿	发烧、肌肉疼痛
A01267	王五	56	结核	咳嗽、发烧

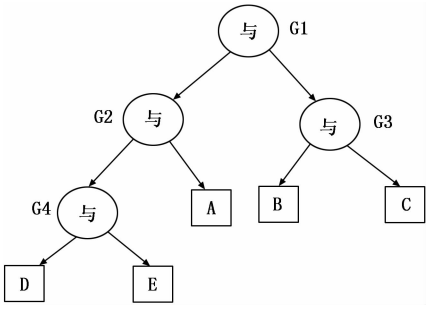

图 2 访问树结构示意图

访问树中的每个内部节点都是阈值门，叶节点是一个属性。如果 x 是叶节点，则使用 parent（x）表示节点 x 的父级，使用 att（x）表示 x 的属性。根据为组创建定义的 POSET 构建树 T。

例如，为表 1 定义了 4 组，即 G_1、G_2、G_3 和 G_4。根据树 T 树，每个组有 $G_1=\{A,B,C,D,E\}$，$G_2=\{A,D,E\}$，$G_3=\{B,C\}$，$G_4=\{D,E\}$ 个属性集。根据 POSET 的定义，$G_2\leqslant G_1$ 表示 G_1 的访问权限大于 G_2。在这里，G_1 是可以查看所有属性的最大根组。每个组都可以查看其属性及其子组的属性。

由于使用 CP－ABE 对整个数据库进行加密涉及许多昂贵的双线性对操作[12-16]，从而导致较高的计算开销，因此使用对称加密对 EMR 数据库进行加密。对称加密所需的计算时间小于 CP－ABE。因此，提出的 G－CP－ABE 分为两个加密阶段。在阶段 1 中，EMR 数据库使用健壮的对称加密（AES－256 位密钥）进行加密，而在阶段 2 中，使用 CP－ABE 对用于对称加密的密钥进行加密。因此，两级加密大大减少了计算时间和计算开销。

基于访问树 T，选择对称加密的随机密钥。以图 2 中的访问树为例，键值选择为 $G_4\leftarrow k_1$，$G_3\leftarrow k_2$，$G_2\leftarrow(k_1,k_3)$，$G_4\leftarrow(k_1,k_2,k_3)$。该分配意味着数据库的字段 $\{D,E\}$ 使用 k_1 加密，$\{B,C\}$ 使用 k_2 加密，$\{A\}$ 使用 k_1 加密。密钥表的构造如表 2 所示。

表 2 秘钥表

G_1	G_2	G_3	G_4
$\{\{k_1\},\{k_2\},k_3\}$	$\{\{k_1\},k_3\}$	$\{k_2\}$	$\{k_1\}$

密钥表指示组之间的部分排序。组 G_4 只能解密密钥 k_1，并且可以解密和查看属性 $\{D,E\}$，而组 G_1 可以解密所有密钥，并且可以查看数据库的所有属性。按照 POSET 的构造，创建修改后的访问树，如图 3 所示。

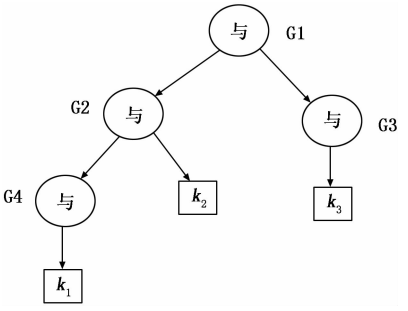

图 3 修改后的访问树

根据表 2 中的密钥表绘制访问树。与图 2 所示的原始访问树相比，修改后的访问树对叶节点的数量进行了优化。由于双线性对的数量与叶节点的数量成正比，因此叶节点数量的减少是非常有利的。在实际情况中，EMR 表有许多属性，修改后的访问树结构使 G－CP－ABE 能够更快地执行加密和解密。CP－ABE 的解密时间在很大程度上取决于访问树中叶节点的数量，计算时间明显缩短。

当用户希望搜索一个或多个数据字段时，应该将对应于组标识的密钥 SKS 发送到云服务器。如果密钥 SKS 满足各个组的访问结构，则服务器返回加密的数据库表。数据用户运行解密算法以获得所需的解密密钥。

然后，EMR 所有者使用 CPABE 方案对密钥表 K 进行加密，并将访问策略嵌入到密钥表的密文中。密钥表的属性是随机对称密钥。随机密钥的数量总是有限的，因为它直接取决于组的数量。对于表 1 的数据，组数为 4，秘钥数为 3。因此，秘钥的数量总是小于或等于组的数量。结果，属性的数量减少了。由于双线性配对操作的数量和加密密钥的长度取决于表中属性的数量，所以属性的减少总是会减少提供性能增强所涉及的计算。另外，不加密原始表，而是使用 CP－ABE 对简化后的小密钥表进行加密，从而最小化总的加密和解密时间。

解密过程相对简单。数据用户从 EMR 云下载密文文件 C。该文件有两部分。第一部分存储密钥表 K 的密文，用户对这一部分进行解密，获得所需的匹配组属性集的相应对称解密密钥。。

2.2 G－CP－ABE 结构

用户的私钥由给定的组属性集标识。使用一个希函数 $H:\{0,1\}^*\rightarrow G_0$，将属性的二进制表示映射到一个随机的组元素。属性集合被定义为 $U=\{A_1,A_2,\cdots,A_n\}$。除了 CP－ABE 方案的各个阶段之外，所提出的 G－CP－ABE 方案还包括对称密钥设置、对称加密和对称解密功能。当数据量较大时，CP－ABE 会产生更多的计算开销。因此，对称加密是实现计算效率的较好选择。

设置 $(1^m,U)\rightarrow(PK,MK)$：TCA 运行 Setup 算法，选

择素数为 p 和生成器为 g 的双线性组 G_0，设置安全参数为 m，并在 Z_p 中选择两个随机元素 α，β。算法输出公钥 PK 和主密钥 MK 如下：

$$PK = \{G_0, g, h = g^{\beta}, e(g,g)^{\alpha}\} \tag{1}$$

$$MK = \{g^{\alpha}, \beta\} \tag{2}$$

密钥生成 $(PK, MK, S) \rightarrow SK_S$：密钥生成算法将 S 作为输入组属性集并输出秘密密钥 SK_S，并用该集合进行标识。该算法为 S 中的每个属性 i 随机选择 $r \in Z_p$ 和 $r_i \in Z_p$。密钥计算如下：

$$SK_S = (D = g^{\alpha} \cdot h^{r}, \forall i \in S: D_i = g^{r} \cdot H(i)^{r_i}, D_i' = h^{r_i}) \tag{3}$$

此时，每个属性集都最少有一个属性，最多有 m 个属性，其中 m 表示使用的随机密钥的总数。属性数越少，越能减少 CP－ABE 密钥的计算量和长度。由于修改后的访问树具有较少数量的属性，因此 G－CP－ABE 花费的密钥生成时间更少。使用修改后的访问树，可以大大减少求幂运算的次数。

数据所有者调用子例程加密 (PK, K, A)。其中，PK 为公钥，K 为对称密钥集，A 为组访问结构。该算法输出密文 C_2。数据使用者只有在拥有正确的属性集时，才可以访问相应的解密密钥。数据所有者从 Z_p 中选择 m 个随机数 $x_1, x_2, \cdots, x_m$，然后计算 C_i^1 和 $C_i^2 (i = 1,2 \cdots m)$。

$$C_i^1 = k_i \cdot e(g,g)^{\alpha \cdot x_i}, C_i^2 = g^{x_i} \tag{4}$$

由于 m 是有限小的，所以 G－CP－ABE 的指数运算次数很少，该算法为访问树中的每个节点 y 选择多项式 q_y。节点信息是从上到下随机选择的。对于每个节点 y，多项式的阶数设置设为 $k_y - 1$，其中 k_y 为该节点的阈值。从根节点 R 开始，数据所有者设置 $q_R(0) = x_1$，并选择其他点来定义多项式 q_R。多项式中的点由两种类型的节点组成：层次节点和从访问树中随机选择的节点。设置 $q_y(0) = q_{parent_y}(index(y))$。考虑叶节点 L 的集合，然后数据所有者对 L 中的每个叶节点 z 计算 $C_i^1(z)$ 和 $C_i^2(z)$，如下所示：

$$C_i^1(z) = h^{q_z(0)}, C_i^2 = H(att(y))q_y(0) \tag{5}$$

此时，集成密钥集密文。对称加密还针对每个属性子集使用 m 个密钥进行迭代执行，最后上传的密文为 $\{C_1, C_2\}$。

解密 (C, SK_S)：数据用户迭代调用这个子例程。与 CP－ABE 类似，定义了一个递归函数解密节点 (C_2, SK_S, y)，它采用 C_2（G－CPE 密文）、用户密钥 SK_S 和一个节点 y。

如果节点 y 是叶节点，则 $i = att(y)$，如果 i 在 S 中，则：

$$DecryptNode(C_2, SK_S, y) = \frac{e(D_i, C_y^1)}{e(D_i', C_y^2)} = \frac{e(g^{r} \cdot H(a_i)^{r_i}, h^{q_y(0)})}{e(g^{r_i} \cdot H(att(y))q_y(0))} = e(g,g)^{r \cdot \beta \cdot q_y(0)}$$

如果 i 不在 S 中，则将 $DecryptNode(C_2, SK_S, y)$ 设置为 null。如果 y 不是叶节点，那么对于 $z = child(y)$ 的每个节点 z，运行 $DecryptNode(C_2, SK_S, y)$ 并将结果存储在 F_z 中。设 S_x 为子节点 z 的任意 k_x 大小的集合，使得 F_z 不为空。如果不存在这样的节点，则表示该节点不满足并返回 null。否则，计算下式：

$$F_y = \prod_{z \in S_y} F_z^{\Delta_i S'_{y(0)}} = \prod_{z \in S_y} (e(g,g)^{r \cdot \beta \cdot q_z(0)})^{\Delta_i S'_{y(0)}} = \prod_{z \in S_y} (e(g,g)^{r \cdot \beta \cdot q_y(i)})^{\Delta_i S'_{y(0)}} = e(g,g)^{r \cdot \beta \cdot q_y(0)}$$

其中：$i = index(z), S'_y = \{index(z): z \in S_y\}$。

如果 S 满足访问树，则设置：

$$A_i = DecryptNode(C_2, SK_S, Y_i) = e(g,g)^{r \cdot \beta \cdot q_z(0)} = e(g,g)^{r \cdot \beta \cdot S_i} (i = 1,2 \cdots k)$$

接下来，可以这样计算 $e(g,g)^{\alpha S_i}$：

$$F_i = \frac{e(C_i^1, D)}{A_i} = \frac{e(g^{S_i} \cdot g^{\alpha} \cdot g^{\beta r})}{e(g,g)^{r \cdot \beta \cdot S_i}} = e(g,g)^{\alpha S_i}$$

CP－ABE 的解密时间取决于用户拥有的属性数量。在此，由于使用 POSET 组结构创建访问树，因此在 G－CP－ABE 中分配给用户的属性数量较少。因此，G－CP－ABE 具有更好的解密性能。

基于层次结构，节点可以确定后继节点（子节点）的密钥，但反之则不成立。如果 S_i 是当前节点，则依次确定 $e(g,g)^{\alpha S_i}, e(g,g)^{\alpha S_{i+1}}, \cdots, e(g,g)^{\alpha S_{i+m}}$ 并获得密钥 $\{k_i, k_{i+1} \cdots k_m\}$。现在，目标组用户可以解密并查看密钥表中的属性 $\{A_i, A_{i+1} \cdots A_m\}$。

$$\frac{C_i^1}{F_i} = \frac{k_i \cdot e(g,g)^{\alpha S_i}}{e(g,g)^{\alpha S_i}} = k_i, i = 1,2 \quad m \tag{10}$$

2.3　紧急访问

通过添加一个默认组策略来处理紧急情况，如图 4 所示。

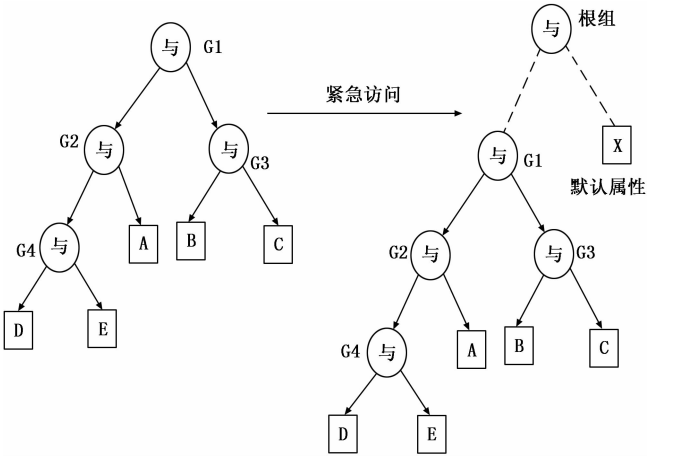

图 4　紧急情况下的访问树更新

添加一个虚拟属性，并将应急组作为访问树的根组。现在，根组有权查看所有属性。根组是使用时间参数创建的，并且在句点之后无效。然后，删除根并保留原始的访问树。修改后的密钥表如表 3 所示。

表 3　修改后的密钥表

根组	G_1	G_2	G_3	G_4
$\{\{k_1\}, \{k_2\}, k_3\}$	$\{\{k_1\}, \{k_2\}, k_3\}$	$\{\{k_1\}, k_3\}$	$\{k_2\}$	$\{k_1\}$

组的创建和管理由数据所有者本身作为访问结构创建的一部分来完成。假设使用简单的组管理，因为 CP－ABE 可以防止串通攻击。

3 安全分析

提出的方案可确保对外包给云的医疗记录的隐私和更好的访问控制。假设端到端通信是通过 SSL、TSL 或任何其他安全协议安全加密的。当且仅当其属性与嵌入在第二个密文中的访问策略匹配时，每个用户可以解密这些记录。

在决策双线性密钥交换算法（DBDH）的假设下，所提出的 EMR 访问控制策略在组访问策略安全模型中是安全的。

4 实际运行分析

为了验证安全性分析，使用 CP－ABE 工具包（斯坦福大学）和基于 Java 配对的密码库实现了 G－CPABE。该实验采用具有 1024 位离散日志安全性的 A 型配对。使用高级加密标准（AES）对 EMR 表进行加密，而 ABE 密文是加密的 AES 密钥。在 3.64 GHz Intel Core i7 处理器，Ubuntu 14.04、14 GB RAM 的处理器上进行了实验。

在仿真初始阶段，该模型建立了基于 POSET 的访问结构，并对属性进行了分组（如图 2 和图 3 所示）。属性的分组创建了一种数据库的逻辑垂直分区。每个逻辑分区都使用随机对称密钥加密。G－CP－ABE 不是使用单个对称密钥，而是使用多个密钥对数据库的每个逻辑片段进行加密，以提供更高的安全性。CP－ABE 的加密时间与访问树中的叶节点数量成正比。仿真中使用的属性数为｛5、10、15、20、25、30、35、40、45 和 50｝。同时，通过改变 EMR 表中的记录数来进行实验。

用于 AES 加密的密钥根据组访问结构存储在密钥表中（见表 2）。然后使用 CP－ABE 方案对密钥表进行加密。密钥生成时间是根据所创建组的键表中的子集数量来度量的。图 5 所示的结果表明，密钥生成时间与各组密钥结构中子集的数量成线性关系。由于修改后的访问树中的叶子节点减少，因此该方法的密钥生成时间更短。

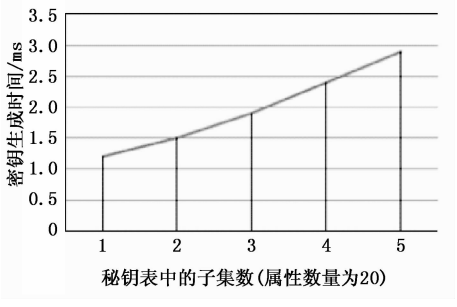

图 5 密钥生成时间与密钥表中的子集

访问结构只考虑“与”门，以确保所有属性都参与访问策略的创建。测量访问树中的级别对加密时间的影响，结果如图 6 所示，表明加密时间随访问树中级别的数量线性增加。

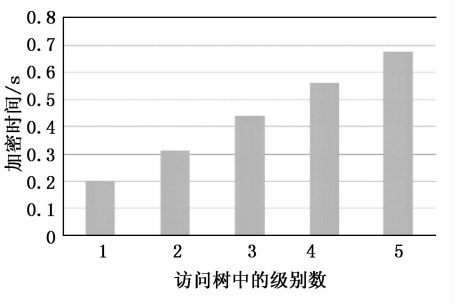

图 6 加密时间与访问树的深度

所提出的模型通过使用基于 POSET 的组结构来减少访问树的深度，从而显着减少了总体加密时间。使用不同数量的记录进行仿真，加密时间随记录数量的增加而线性增加。结果如图 7 所示。使用基于 POSET 的组访问结构对原始访问树进行优化。优化过程减少了访问树中的叶节点数量，从而改进了密钥生成、加密和解密性能。

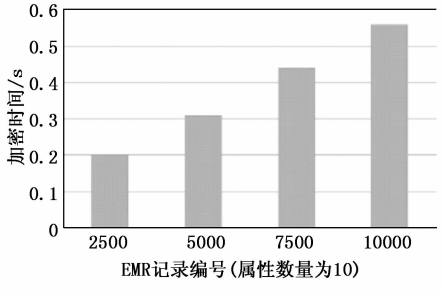

图 7 加密时间与 EMR 记录的数量

5 结论

结合 AES 和 CP－ABE 加密标准，提出了一种新的具有显著计算增益的细粒度访问结构 G－CP－ABE。POSET 通过对用户进行分组来创建访问结构，并将属性分配给组而不是个人。G－CP－ABE 的主要优点是与现有作品相比具有最小的双线性对。安全性分析和实验分析表明，改进的 G－CP－ABE 性能使该方案适用于云和资源受限的物联网设备。

参考文献：

[1] 鲍灵燕，梁世健. 互联网技术在医疗设备管理中的应用 [J]. 山东工业技术，2017 (12)：157－157.

[2] 胡亚荣. 新互联网时代医疗设备分销渠道设计及渠道管理决策的研究 [J]. 内蒙古财经大学学报，2017，15 (4)：51－55.

[3] 申 超. 面向大数据应用的云计算中心性能分析方法 [D]. 上海：上海大学，2017.

[4] 关志涛，杨亭亭，徐茹枝，等. 面向云存储的基于属性加密的多授权中心访问控制方案 [J]. 通信学报，2015，36 (6)：116－126.

[5] 王光波，王建华. 基于属性加密的云存储方案研究 [J]. 电子与信息学报，2016，38 (11)：2931－2939.

(下转第 209 页)