个人健康记录云管理系统中支持用户撤销的细粒度访问控制

刘 琴*① 刘旭辉① 胡柏霜① 张少波②③
①(湖南大学信息科学与工程学院 长沙 410082)
②(中南大学信息科学与工程学院 长沙 410083)
③(湖南科技大学计算机科学与工程学院 湘潭 411201)

摘 要：随着云计算的发展，越来越多的用户在使用个人健康记录(PHR)云管理系统，由于 PHR 包含了患者的隐私信息，因此一般在将 PHR 上传到云平台之前会先对其进行加密。基于比较的加密(CBE)在基于属性的访问策略中实现了时间比较，然而 CBE 加密时间与访问策略中的属性数目线性增长，从而导致其开销过大；同时，方案难以实时撤销用户的访问权限。该文提出支持用户撤销的细粒度访问控制(FGUR)方案，通过将属性层次引入到 CBE 中，同时结合广播密文策略的基于属性加密(BCP-ABE)，高效地实现 PHR 云管理系统中的细粒度访问控制及用户实时撤销。实验结果表明，与 CBE 相比，FGUR 方案在加密开销和动态访问权限方面具有更好的性能。

关键词：云计算；个人健康记录；基于比较的加密；属性层次；用户撤销
中图分类号： TP393 **文献标识码**： A **文章编号**：1009-5896(2017)05-1206-07
DOI: 10.11999/JEIT160621

Fine-grained Access Control with User Revocation in Cloud-based Personal Health Record System

LIU Qin① LIU Xuhui① HU Baishuang① ZHANG Shaobo②③
①(*College of Computer Science and Electronic Engineering*, *Hunan University*, *Changsha* 410082, *China*)
②(*School of Information Science and Engineering*, *Central South University*, *Changsha* 410083, *China*)
③(*School of Computer Science and Engineering*, *Hunan University of Science and Technology*, *Xiangtan* 411201, *China*)

Abstract: With the development of cloud computing, more and more users employ cloud-based Personal Health Record (PHR) systems. The PHR is correlated with patient privacy, thus existing research suggests to encrypt PHRs before outsourcing. Comparison-Based Encryption (CBE) realizes time comparison in attribute-based access policy, however, the time for encryption is linearly with the number of attributes in the access policy. Therefore, the cost of the scheme is extensive; besides, the scheme is difficult to revoke the user's access privileges in real time. To realize efficiently a fine-grained access control and user revocation for PHRs in clouds, a Fine-Grained access control with User Revocation (FGUR) scheme is proposed by incorporating Broadcast Ciphertext-Policy Attribute-Based Encryption (BCP-ABE) and an attribute hierarchy into CBE. The experiment results show that the FGUR scheme has better performance in terms of the encryption cost and dynamic access privilege, compared with CBE.

Key words: Cloud computing; Personal Health Record (PHR); Comparison-Based Encryption (CBE); Attribute hierarchy; User revocation

1 引言

近年来，个人健康记录(Personal Health Record, PHR)系统作为一种以患者为中心的医疗信息交流平台越来越受到用户的欢迎[1]。PHR可以使医务人员在线访问一个患者的完整医疗记录，从而能更加高效准确地为其制定医疗方案[2]。云计算是一种新兴的网络应用模式，它将大量计算资源和存储资源连接在一起，形成巨大的虚拟资源共享池为用户提供服务[3]。由于其高可靠性，动态扩展性和低成本等优点，越来越多的患者将其PHR上传到云中，从而可以使用智能终端设备随时随地访问云中数据。然而，PHR与患者的隐私紧密相关，它包含大量以患者为

收稿日期：2016-06-12；改回日期：2016-12-07；网络出版：2017-01-22
*通信作者：刘琴 gracelq628@hnu.edu.cn
基金项目：国家自然科学基金(61632009, 61402161)，湖南省科技厅项目(2015JJ3046)，赛尔网络下一代互联网技术创新项目(NGII 20150408)
Foundation Items: The National Natural Science Foundation of China (61632009, 61402161), The Hunan Provincial Natural Science Foundation of China (2015JJ3046), The CERNET Innovation Project (NGII20150408)

中心的医疗数据，如过敏、家族病史、影像报告(如X射线)等。如果让云服务提供商(Cloud Service Provider, CSP)来管理这些敏感的医疗数据，可能会引起潜在的安全问题。例如，CSP可能会为了牟利而故意将PHR泄露给医药公司或医疗器械公司[4]。

为保护患者的PHR隐私，目前国内外学者已提出一些保护方法。例如，文献[5]利用基于属性加密(Attribute-Based Encryption, ABE)，为整体医疗保障系统提出了一个基于混合云的框架，通过混合云来确保医疗数据转移和整合的安全性。为了实现对PHR的细粒度访问控制及可扩展的数据控制，文献[6]利用基于优先级的加密(Prioritized Level Based Encryption, PLBE)技术加密PHR文件。文献[7]针对多数据源的PHR云管理系统，利用保序对称加密(Order Preserving Symmetric Encryption, OPSE)[8]来保护数据隐私。目前大部分研究方案都采用ABE作为密码学工具，实现云管理系统中的细粒度访问控制[9,10]。

在ABE的基础上，Zhu等人[11]提出了基于比较的加密(Comparison-Based Encryption, CBE)方案，该方案利用前向和后向导出函数实现了基于属性访问策略中的时间比较。然而，CBE的加密开销随着访问策略的复杂性线性增长，其次，CBE难以实时撤销一个用户的访问权限。针对以上问题，本文提出支持用户撤销的细粒度访问控制(Fine-Grained access control with User Revocation, FGUR)方案。该方案为属性建立一个层次结构，其上层属性是下层属性的泛化，并利用少量的上层泛化属性加密密文，提高加密效率。为实现属性层次，FGUR方案首先使用正/逆向深度优先(Positive-Negative Depth-First , PNDF)编码对属性树中的每个结点进行编码。然后，应用CBE中的后向导出函数，使子孙属性结点能够推导出其祖先结点所关联的密钥，从而拥有具体属性的用户可以解密由泛化属性所加密的密文。为实现动态访问权限，FGUR方案结合广播密文策略的基于属性加密(Broadcast Ciphertext Policy-Attribute Based Encryption, BCP-ABE)[12]，将合法用户标识集(W)融入基于属性的访问策略中，使只有标识(ID)位于W中且属性满足访问策略的用户才能解密密文。同时，当一个用户被撤销时，系统只需将该用户ID从W中删除，无需为合法用户重新分配密钥，从而提高撤销用户权限的效率。

本文主要贡献和创新点如下：(1)将属性层次引入到CBE方案中，高效地实现PHR云管理系统中的细粒度访问控制；(2)结合BCP-ABE，实现用户访问权限的实时撤销，保证动态访问控制的正确性；(3)分析了FGUR方案的性能和安全性，并通过实验验证它的有效性和高效性。

2　系统模型及相关定义

2.1 系统模型

系统主要由以下3部分组成：云服务提供商(CSP)、数据拥有者以及数据用户(简称用户)。云服务商提供云存储环境，运行PHR云管理系统，在线管理用户的存储数据。数据拥有者是利用PHR云管理系统管理其个人健康记录的病人。用户是由数据拥有者授权的，可访问云中数据的实体。此外，当所有用户位于同一个可信域时，可在可信域的内部部署一个负责部分解密操作的代理服务器。

设合法用户标识集$W=U\setminus R$，其中$U=[n]=\{1,2,\cdots,n\}$为系统中用户的标识域，R为用户撤销列表，包含被撤销用户的ID。设全局属性集为$\mathcal{A}=\{A_1,A_2,\cdots,A_m\}$，根据该属性集建立一个$L$层的属性层次$\widehat{\mathcal{A}}$，其中，每个属性$A_k$包含两个层次编码$\{\mathrm{Pcode}_k,\mathrm{Ncode}_k\}$，且子孙结点的编码大于其祖先结点的编码。在使用PHR云管理系统时，为了能高效地实现细粒度访问控制和用户实时撤销，FGUR方案利用精确ID和基于属性的访问权限$\widehat{\mathcal{L}}$来表示每个用户，即标识为ID(ID$\in U$)的用户访问权限为$(\mathrm{ID},\widehat{\mathcal{L}})$，其中每个属性$A_k\in\widehat{\mathcal{L}}$与用户的授权时间$[t_a,t_b]$和层次编码$\{\mathrm{Pcode}_k,\mathrm{Ncode}_k\}$相关，记作$A_k(t_a,t_b,\mathrm{Pcode}_k,\mathrm{Ncode}_k)$。同时，FGUR方案利用合法用户标识集$W$和基于属性的访问策略$\widehat{\mathrm{AP}}$来加密PHR，即PHR的访问策略表示为$(W,\widehat{\mathrm{AP}})$，其中，每个属性$A_l\in\widehat{\mathrm{AP}}$，与时间条件$[t_i,t_j]$和层次编码$\{\mathrm{Pcode}_l,\mathrm{Ncode}_l\}$相关，记作$A_l(t_i,t_j,\mathrm{Pcode}_l,\mathrm{Ncode}_l)$。当系统中某用户被撤销时，数据拥有者首先将该用户ID添加到集合R中，同时更新集合$W'=W\setminus\mathrm{ID}$，然后利用该撤销用户的ID生成一个更新密钥UKID，并将UKID发送给云服务提供商，云服务提供商将密文的访问策略更新为$(W',\widehat{\mathrm{AP}})$。

2.2 攻击模型

FGUR方案的设计目标是保护数据拥有者在使用PHR云管理系统时的个人数据隐私。主要存在两种攻击：由未经授权的外来者所发起的外部攻击，以及由诚实而好奇的CSP和不可信的用户所发起的内部攻击。在现有的SSL和SSH等安全协议保护下，本文假设通信渠道是安全的，因此主要考虑内部攻击。设诚实而好奇的CSP总是正确地执行一个给定的协议，但可能会试图了解一些与所存数据有

关的额外信息；同时，不可信用户可能会相互串谋，伪造解密密钥，从而解密出非授权的数据。因此，若以下任意一种情形发生，则 FGUR 方案被认为不安全：

情形 1：当下列任一条件成立时，拥有访问权限 $(\mathrm{ID},\widehat{\mathcal{L}})$ 的用户 uk 可以访问其访问策略为 $(W,\widehat{\mathrm{AP}})$ 的 PHR;

(1) $\widehat{\mathcal{L}} \not\subseteq \widehat{\mathrm{AP}}$; (2) $[t_a,t_b]\cap[t_i,t_j]=\mathrm{null}$;

(3) $(\mathrm{Pcode}_k < \mathrm{Pcode}_l)\vee(\mathrm{Ncode}_k < \mathrm{Ncode}_l)$

(4) $\mathrm{ID}\notin W$ 。

情形 2：CSP 能够在没有权限的情况下解密 PHR。

3 FGUR 方案

根据属性集合 $\mathcal{A}=\{A_1,A_2,\cdots,A_m\}$, FGUR 方案构建了一个 L 层的属性层次 $\widehat{\mathcal{A}}$，如图 1(a)所示。在属性树中，较上层属性是较下层属性的抽象。采用深度优先遍历算法为每个属性节点分别生成两个层次编码：正向编码 Pcode 和逆向编码 Ncode。设每个结点有 4 个域：Pcode, Ncode, rchild (右子树),, lchild(左子树)。算法首先将根节点 Root 压入到 PStack 和 NStack 两个栈。在 PStach 中，每个节点的右子树将首先被压入，因此，左子树的正向编码要大于右子树的正向编码。相反地，在 NStack 中，每个节点的左子树将首先被压入，因此，右子树的逆向编码要大于左子树的逆向编码。

以图 1(a)中的属性树为例，其 PNDF 编码如图 1(b)和图 1(c)所示。设 Pcode_i 和 Ncode_i 分别代表节点 i 的 Pcode 和 Ncode。如果节点 i 是节点 j 的子孙节点，那么 PNDF 编码具有如下特性：$\mathrm{Pcode}_i > \mathrm{Pcode}_j$，$\mathrm{Ncode}_i > \mathrm{Ncode}_j$。例如，属性 Surgery 的 Pcode 和 Ncode 分别是 2 和 5；属性 Heart Srugery 的 Pcode 和 Ncode 分别是 3 和 7；属性 Respiratory Medicine 的 Pcode 和 Ncode 分别是 6 和 4。Heart Srugery 作为 Surgery 的子节点，它的 Pcode 和 Ncode 均比 Surgery 的大。而 Respiratory Medicine 不是 Surgery 的子节点，因此，它的 Ncode 比 Surgery 的小。

设属性层次中的节点数是 m。在 FGUR 中，层次编码被表示成一组离散值 $U_m=\{(\mathrm{Pcode}_1,\mathrm{Ncode}_1),(\mathrm{Pcode}_2,\mathrm{Ncode}_2),\cdots,(\mathrm{Pcode}_k,\mathrm{Ncode}_k),\cdots,(\mathrm{Pcode}_m,\mathrm{Ncode}_m)\}$, $0\le\mathrm{Pcode}_1\le\mathrm{Pcode}_2\le,\cdots,\le\mathrm{Pcode}_m\le Z_m$,$0\le\mathrm{Ncode}_1\le\mathrm{Ncode}_2\le\cdots,\le\mathrm{Ncode}_m\le Z_m$，其中 Z_m 是最大的整数。FGUR 利用文献[11]提出的后向导出函数 (Backward Derivation Function, BDF)来实现属性层次。设 $G_{n'}$ 是合数阶 $n'=p'q'$ 的乘法群，其中 $p'q'$ 是两个大素数。首先，在 $G_{n'}$ 中选择两个唯一的随机生成元 φ_1,φ_2，在 $Z_{n'}^*$ 中选择两个唯一的随机数 θ_1,θ_2，其中，在 $Z_{n'}^*$ 中，θ_1,θ_2 的阶足够大。然后，定义两个映射函数 $\psi_1(\cdot),\psi_2(\cdot)$，负责将整数集 $U_m=\{(\mathrm{Pcode}_1,\mathrm{Ncode}_1),\cdots,(\mathrm{Pcode}_k,\mathrm{Ncode}_k),\cdots,(\mathrm{Pcode}_m,\mathrm{Ncode}_m)\}$ 映射到 $V_m=\{(v_{\mathrm{Pcode}_1},v_{\mathrm{Ncode}_1}),\cdots,(v_{\mathrm{Pcode}_k},v_{\mathrm{Ncode}_k}),\cdots,(v_{\mathrm{Pcode}_m},v_{\mathrm{Ncode}_m})\}$，具体定义为

$$\left.\begin{aligned} v_{\mathrm{Pcode}_k}&=\psi_1\left(\mathrm{Pcode}_k\right)=\varphi_1^{\theta_1^{Z_m-\mathrm{Pcode}_k}}\\ v_{\mathrm{Ncode}_k}&=\psi_2\left(\mathrm{Ncode}_k\right)=\varphi_2^{\theta_2^{Z_m-\mathrm{Ncode}_k}}\end{aligned}\right\} \tag{1}$$

根据 $\psi_1(\cdot),\psi_2(\cdot)$ 的定义，后向导出函数 $f_1(\cdot),f_2(\cdot)$ 的定义为

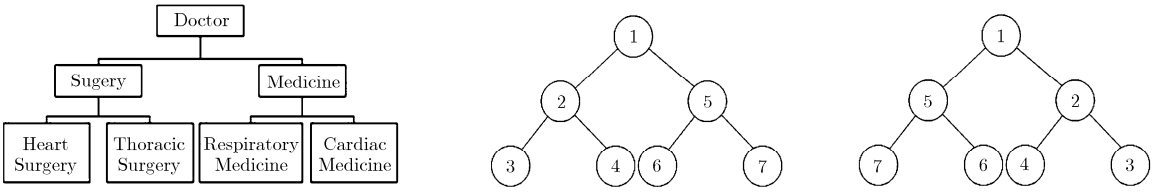
$$\left.\begin{aligned} v_{\mathrm{Pcode}_j}&\leftarrow f_1\left(v_{\mathrm{Pcode}_k}\right)=\left(v_{\mathrm{Pcode}_k}\right)^{\theta_1^{\mathrm{Pcode}_k-\mathrm{Pcode}_j}},\\ &\quad\ \mathrm{Pcode}_k\ge\mathrm{Pcode}_j\\ v_{\mathrm{Ncode}_j}&\leftarrow f_2\left(v_{\mathrm{Ncode}_k}\right)=\left(v_{\mathrm{Ncode}_k}\right)^{\theta_2^{\mathrm{Ncode}_k-\mathrm{Ncode}_j}},\\ &\quad\ \mathrm{Ncode}_k\ge\mathrm{Ncode}_j\end{aligned}\right\} \tag{2}$$

4 FGUR 方案的构造

FGUR 由以下 8 个算法构成：

(1) $\mathrm{Setup}\left(1^\kappa,\widehat{\mathcal{A}}\right)\rightarrow\left(\mathrm{MK},\mathrm{PK}_{\widehat{\mathcal{A}}}\right)$：给定双线性映射系统 $S_N=(N=pq,G,G_T,e)$，其中 G,G_T 是合数阶 $n=sn'$ 的循环群，并且 $e:G\times G\rightarrow G_T$。算法首先随机选取生成元 $\omega\in G,g\in G_s$，以及 $\varphi,\overline{\varphi},\varphi_1,\varphi_2\in G_{n'}$,其中 G_s 和 $G_{n'}$ 是群 G 的两个子群。因此，可得 $e(g,\varphi)=e(g,\overline{\varphi})=e(g,\varphi_1,)=e(g,\varphi_2)=1$，而 $e(g,\omega)\ne 1$。

然后，算法选择随机数 $\lambda,\mu,\theta_1,\theta_2\in Z_n^*$，并使用哈希函数 $H:\{0,1\}^*\rightarrow G$ 将二进制字符串所表示的



(a)属性树 (b)正向深度优先编码 (c)逆向深度优先编码

图 1 PNDF 编码

根属性 Root 映射为群中一个随机元素。另外，选择随机指数 $\alpha,\beta,\gamma\in Z_n^*$，设 $h=\omega^{\beta},\eta=g^{1/\beta},\zeta_1=e(g,\omega)^{\alpha},\zeta_2=e(\omega_n,\omega_1),v=\omega^{\gamma}$。选择随机数 $f,c\in Z_n^*$，计算：$\omega_i=\omega^{(f^i)}\in G,(i=1,2,\cdots,n,n+2,\cdots,2n),C_1=\omega^c,C_2=\left(v\prod_{j\in W}\omega_{n+1-j}\right)^c$。

最后，算法输出主密钥：$\mathrm{MK}=(g^{\alpha},\beta,p,q,n',f,\gamma,c)$，和公共密钥：$\mathrm{PK}_{\widehat{\mathcal{A}}}=(S_N,\omega,g,\varphi,\overline{\varphi},\varphi_1,\varphi_2,h,\eta,\zeta_1,\zeta_2,\lambda,\mu,\theta_1,\theta_2,H,v,C_1,C_2,\omega_1,\cdots,\omega_n,\omega_{n+2},\cdots,\omega_{2n})$。

(2) $\mathrm{GenKey}(\mathrm{MK},\mathrm{uk},\widehat{\mathcal{L}},\mathrm{ID})\to\mathrm{SK}_{\widehat{\mathcal{L}}}$：给定拥有属性权限 $\widehat{\mathcal{L}}$ 的用户 uk 及该用户 $\mathrm{ID}\in U,(U=\lfloor u\rfloor=\{1,\cdots,n\})$，选择随机数 $\tau_{\mathrm{uk}},r\in Z_n^*$，对每个属性 $A_k[t_a,t_b,\mathrm{Pcode}_k,\mathrm{Ncode}_k\in\widehat{\mathcal{L}}]$，计算：

$$\begin{aligned}D_{A_k}&=\left(D_t,D_{t_a}^{'},\overline{D}_{t_b}^{'},D_t^{''},D_{K_1},D_{K_2}\right)\\&=\left(g^{\tau_{\mathrm{uk}}}H_{A_k}^r,\left(v_{t_a}\right)^r,(\overline{v}_{t_b})^r,\omega^r,\left(v_{\mathrm{Pcode}_k}\right)^r,\left(v_{\mathrm{Ncode}_k}\right)^r\right)\end{aligned}\tag{3}$$

其中，$H_{A_k}=H(R)\cdot v_{\mathrm{Pcode}_k}\cdot v_{\mathrm{Ncode}_k},v_{t_a}=\varphi^{\lambda^{t_a}},\overline{v}_{t_b}=\overline{\varphi}^{\mu^{Z-t_b}},v_{\mathrm{Pcode}_k}=\varphi_1^{\theta_1^{Z_m-\mathrm{Pcode}_k}}$，以及 $v_{\mathrm{Ncode}_k}=\varphi_2^{\theta_2^{Z_m-\mathrm{Ncode}_k}}$。然后，uk 的私钥设置为

$$\mathrm{SK}_{\widehat{\mathcal{L}}}=\left(D=g^{(\alpha+\tau_{\mathrm{uk}})/\beta},D_1=\omega^{f^{\mathrm{ID}}\gamma},\left\{D_{A_k}\right\}_{A_k\in\widehat{\mathcal{L}}}\right)\tag{4}$$

(3) $\mathrm{Encrypt}\left(\mathrm{PK}_{\widehat{\mathcal{A}}},\widehat{\mathrm{AP}},W\right)\to\left(\widehat{\mathcal{H}}_{\mathcal{P}},\mathrm{ek}\right)$：给定一个关于访问策略 $\widehat{\mathrm{AP}}$ 的访问策略树 $\mathcal{T}$，以及用户下标集 $W\subseteq U$，计算并输出密文头 $\widehat{\mathcal{H}}_{\mathcal{P}}$：

$$\begin{aligned}\widehat{\mathcal{H}}_{\mathcal{P}}=\Big(&\mathcal{T},C=h^{\sigma},C_1,C_2,\left\{\left(\overline{E}_{t_i},E_{t_i}^{'}\right),\left(E_{t_j},E_{t_j}^{'}\right),\right.\\&\left(E_{\mathrm{Pcode}_l},E_{\mathrm{Pcode}_l}^{'}\right),\\&\left.\left.\left(E_{\mathrm{Ncode}_l},E_{\mathrm{Ncode}_l}^{'}\right)\right\}_{A_l[t_i,t_j,\mathrm{Pcode}_l,\mathrm{Ncode}_l]\in T}\right)\end{aligned}\tag{5}$$

各部分设置为

$$\begin{aligned}&\left(\overline{E}_{t_i},E_{t_i}^{'}\right)=\left((\overline{v}_{t_i}\omega)^x,H_{A_l}^x\right),\left(E_{t_j},E_{t_j}^{'}\right)=\left(\left(v_{t_j}\omega\right)^y,H_{A_l}^y\right),\\&\left(E_{\mathrm{Pcode}_l},E_{\mathrm{Pcode}_l}^{'}\right)=\left(\left(v_{\mathrm{Pcode}_l}\cdot\omega\right)^{z_1},H_{A_l}^{z_1}\right),\\&\left(E_{\mathrm{Ncode}_l},E_{\mathrm{Ncode}_l}^{'}\right)=\left(\left(v_{\mathrm{Ncode}_l}\cdot\omega\right)^{z_2},H_{A_l}^{z_2}\right)\end{aligned}\tag{6}$$

其中，$H_{A_l}=H(\mathrm{Root})\cdot v_{\mathrm{Pcode}_l}\cdot v_{\mathrm{Ncode}_l}$。

会话密钥 ek 被设置为 $\mathrm{ek}=\mathrm{ek}_1\cdot\mathrm{ek}_2$，其中 $\mathrm{ek}_1=\zeta_1^{\sigma}=e(g^{\alpha},\omega)^{\sigma},\mathrm{ek}_2=\zeta_2^{c}=e(\omega_n,\omega_1)^c$，$\sigma$ 是主秘密，并且 $\Delta_{\sigma}(A_l)=x+y+z_1+z_2$ 是树 $\mathcal{T}$ 中 σ 的关于属性 A_l 的秘密分享值。

(4) $\mathrm{Delegate}\left(\mathrm{SK}_{\widehat{\mathcal{L}}},\widehat{\mathcal{L}}'\right)\to\mathrm{SK}_{\widehat{\mathcal{L}}'}$：给定私钥 $\mathrm{SK}_{\widehat{\mathcal{L}}}$，一个指定的 $\widehat{\mathcal{L}}'$，对于每个属性 $A_l[t_i,t_j,\mathrm{Pcode}_l,\mathrm{Ncode}_l]\in\widehat{\mathcal{L}}',A_k[t_a,t_b,\mathrm{Pcode}_k,\mathrm{Ncode}_k]\in\widehat{\mathcal{L}}$，算法检测是否 A_l 是 A_k 的泛化属性，以及 $t_a\le t_j$，$t_b\le t_i$。如果满足条件，则计算：

$$\left.\begin{aligned}D_t^{'}&=g^{\tau_{\mathrm{uk}}}H_{A_k}^r\cdot\frac{f_1(D_{K_1})\cdot f_2(D_{K_2})}{\left(v_{\mathrm{Pcode}_k}\right)^r\cdot\left(v_{\mathrm{Pcode}_k}\right)^r}\\&=g^{\tau_{\mathrm{uk}}}H(\mathrm{Root})^r\cdot v_{\mathrm{Pcode}_l}^r\cdot v_{\mathrm{Ncode}_l}^r=g^{\tau_{\mathrm{uk}}}H_{A_l}^r\\D_{t_j}^{'}&\leftarrow f\left(D_{t_a}^{'}\right)\cdot D_t^{''}=f\left(\left(v_{t_a}\right)^r\right)\cdot\omega^r=\left(v_{t_j}\right)^r\cdot\omega^r\\\overline{D}_{t_i}^{'}&\leftarrow\overline{f}\left(\overline{D}_{t_b}^{'}\right)\cdot D_t^{''}=\overline{f}\left((\overline{v}_{t_b})^r\right)\cdot\omega^r=(\overline{v}_{t_i})^r\cdot\omega^r\\D_{\mathrm{Pcode}_l}^{'}&\leftarrow f_1\left(D_{K_1}\right)\cdot D_t^{''}=f_1\left(\left(v_{\mathrm{Pcode}_k}\right)^r\right)\cdot\omega^r\\&=\left(v_{\mathrm{Pcode}_l}\right)^r\cdot\omega^r\\D_{\mathrm{Ncode}_l}^{'}&\leftarrow f_2\left(D_{K_2}\right)\cdot D_t^{''}=f_2\left(\left(v_{\mathrm{Ncode}_k}\right)^r\right)\cdot\omega^r\\&=\left(v_{\mathrm{Ncode}_l}\right)^r\cdot\omega^r\end{aligned}\right\}\tag{7}$$

然后，算法选择一个随机数 $\delta\in Z$，并计算：

$$\left.\begin{aligned}\widetilde{D}_t&=D_t^{'}\cdot\left(gH_{A_l}\right)^{\delta}=g^{\tau_{\mathrm{uk}}}H_{A_l}^r\cdot\left(gH_{A_l}\right)^{\delta}\\&=g^{\tau_{\mathrm{uk}}+\delta}H_{A_l}^{r+\delta}=g^{\tau_k^{'}}H_{A_l}^{r'}\\\widetilde{D}_{t_j}^{'}&=D_{t_j}^{'}\cdot\left(v_{t_j}\omega\right)^{\delta}=\left(v_{t_j}\omega\right)^{r'}\\\widetilde{\overline{D}}_{t_i}^{'}&=\overline{D}_{t_i}^{'}\cdot(\overline{v}_{t_i}\omega)^{\delta}=(\overline{v}_{t_i}\omega)^{r'}\\\widetilde{D}_{\mathrm{Pcode}_l}^{'}&=D_{\mathrm{Pcode}_l}^{'}\cdot\left(v_{\mathrm{Pcode}_l}\omega\right)^{\delta}=\left(v_{\mathrm{Pcode}_l}\omega\right)^{r'}\\\widetilde{D}_{\mathrm{Ncode}_l}^{'}&=D_{\mathrm{Ncode}_l}^{'}\cdot\left(v_{\mathrm{Ncode}_l}\omega\right)^{\delta}=\left(v_{\mathrm{Ncode}_l}\omega\right)^{r'}\end{aligned}\right\}\tag{8}$$

其中，$H_{A_l}=H(\mathrm{Root})\cdot v_{\mathrm{Pcode}_l}\cdot v_{\mathrm{Ncode}_l}$，并且 $\tau_k^{'}=\tau_{\mathrm{uk}}+\delta,r'=r+\delta$。最后，导出私钥为

$$\mathrm{SK}_{\widehat{\mathcal{L}}'}=\left\{\widetilde{D}_t,\widetilde{D}_{t_j}^{'},\widetilde{\overline{D}}_{t_i}^{'},\widetilde{D}_{\mathrm{Pcode}_l}^{'},\widetilde{D}_{\mathrm{Ncode}_l}^{'}\right\}_{A_l\in\widehat{\mathcal{L}}'}$$

(5) $\mathrm{Decrypt1}\left(\mathrm{SK}_{\widehat{\mathcal{L}}'},\widehat{\mathcal{H}}_{\mathcal{P}}\right)\to\widehat{\mathcal{H}}_{\mathcal{P}}^{'}$：给定私钥 $\mathrm{SK}_{\widehat{\mathcal{L}}'}$ 和密文头 $\widehat{\mathcal{H}}_{\mathcal{P}}$，算法首先检测每个属性 $A_l\left[t_i,t_j,\mathrm{Pcode}_l,\mathrm{Ncode}_l\right]\in\widehat{\mathcal{L}}'$ 是否与 $A_l\left[t_i,t_j,\mathrm{Pcode}_l,\mathrm{Ncode}_l\right]\in\widehat{\mathrm{AP}}$ 相符合，如果是，则 σ 的秘密分享值 $\Delta_{\sigma}(A_l)$ 可以通过以下算法被重新构建：

$$F_1\leftarrow\frac{e\left(\widetilde{D}_t,\overline{E}_{t_i}\right)}{e\left(\widetilde{\overline{D}}_{t_i}^{'},E_{t_i}^{'}\right)}=\frac{e\left(g^{\tau_k^{'}}H_{A_l}^{r'},(\overline{v}_{t_i}\omega)^x\right)}{e\left((\overline{v}_{t_i}\omega)^{r'},H_{A_l}^x\right)}=e\left(g^{\tau_k^{'}},\omega\right)^x\tag{9}$$

$$F_2\leftarrow\frac{e\left(\widetilde{D}_t,E_{t_j}\right)}{e\left(\widetilde{D}_{t_j}^{'},E_{t_j}^{'}\right)}=\frac{e\left(g^{\tau_k^{'}}H_{A_l}^{r'},\left(v_{t_j}\omega\right)^y\right)}{e\left(\left(v_{t_j}\omega\right)^{r'},H_{A_l}^y\right)}=e\left(g^{\tau_k^{'}},\omega\right)^y\tag{10}$$

$$\begin{aligned}F_3\leftarrow\frac{e\left(\widetilde{D}_t,E_{\mathrm{Pcode}_l}\right)}{e\left(\widetilde{D}_{\mathrm{Pcode}_l}^{'},E_{t_j}^{'}\right)}&=\frac{e\left(g^{\tau_k^{'}}H_{A_l}^{r'},\left(v_{\mathrm{Pcode}_l}\omega\right)^{z_1}\right)}{e\left(\left(v_{\mathrm{Pcode}_l}\omega\right)^{r'},H_{A_l}^{z_1}\right)}\\&=e\left(g^{\tau_k^{'}},\omega\right)^{z_1}\end{aligned}\tag{11}$$

$$F_4 \leftarrow \frac{e\left(\widetilde{D}_t, E_{\mathrm{Ncode}_l}\right)}{e\left(\widetilde{D}'_{\mathrm{Ncode}_l}, E'_{t_j}\right)} = \frac{e\left(g^{\tau'_k} H_{A_l}^{r'}, \left(v_{\mathrm{Ncode}_l}\omega\right)^{z_2}\right)}{e\left(\left(v_{\mathrm{Ncode}_l}\omega\right)^{r'}, H_{A_l}^{z_2}\right)}$$
$$= e\left(g^{\tau'_k}, \omega\right)^{z_2} \tag{12}$$

$$F_t = F_1 \cdot F_2 \cdot F_3 \cdot F_4 = e\left(g^{\tau'_k}, \omega\right)^{\Delta_\sigma(A_l)} \tag{13}$$

其中，$H_{A_l} = H(\mathrm{Root}) \cdot v_{\mathrm{Pcode}_l} \cdot v_{\mathrm{Ncode}_l}$。由于 $g^{\tau'_k} \in G_s$，并且 $v_{t_j}^x, \overline{v}_{t_i}^y, v_{\mathrm{Pcode}_l}^{z_1}, v_{\mathrm{Ncode}_l}^{z_2} \in G_{n'}$，因此，$e\left(g^{\tau'_k}, v_{t_j}^x\right) = e\left(g^{\tau'_k}, \overline{v}_{t_i}^y\right) = e\left(g^{\tau'_k}, v_{\mathrm{Pcode}_l}^{z_1}\right) = e\left(g^{\tau'_k}, v_{\mathrm{Ncode}_l}^{z_2}\right) = 1$。然后，利用拉格朗日插值算法，值 $C_3 = \left(g^{\tau'_k}, \omega\right)^{\sigma}$ 可以由 $\left\{e\left(g^{\tau'_k}, \omega\right)^{\Delta_\sigma(A_l)}\right\}_{A_l \in \mathcal{T}}$ 计算获得。最后，输出新的密文头 $\widehat{\mathcal{H}}'_{\mathcal{P}} = \left(C = h^{\sigma}, C_1, C_2, C_3\right)$。

(6) $\mathrm{Decrypt2}\left(\mathrm{SK}_{\widehat{\mathcal{L}}}, \widehat{\mathcal{H}}'_{\mathcal{P}}\right) \rightarrow \mathrm{ek}$：接收到 $\widehat{\mathcal{H}}'_{\mathcal{P}} = \left(C, C_1, C_2, C_3\right)$ 后，用户首先计算：$D' = D \cdot \eta^{\delta}$，然后计算：

$$\mathrm{ek}_1 = \frac{e(C, D')}{C_3},$$
$$\mathrm{ek}_2 = \frac{e\left(\omega_{\mathrm{ID}}, C_2\right)}{e\left(\prod_{\substack{j \in W \\ j \neq \mathrm{ID}}} \omega_{n+1-j+\mathrm{ID}}, C_1\right)} \cdot \frac{1}{e(C_1, D_1)} \tag{14}$$

最后，计算出会话密钥 $\mathrm{ek} = \mathrm{ek}_1 \cdot \mathrm{ek}_2$

(7) RevokeUser(ID,MK,pk)：当发生用户撤销时，数据拥有者运行用户撤销算法，接收被撤销的用户 ID 作为输入，输出更新密钥 $\mathrm{UKID} = \left(\omega_{n+1-\mathrm{ID}}\right)^c = \left(\omega^{(f^{n+1-\mathrm{ID}})}\right)^c$。

(8) $\mathrm{CTUpdate}(\mathrm{UKID}, \widehat{\mathcal{H}}_{\mathcal{P}}) \rightarrow \left[\widehat{\mathcal{H}}_{\mathcal{P}}\right]$：云存储中心输入更新密钥 UKID，使用式(15)对密文头 $\widehat{\mathcal{H}}_{\mathcal{P}}$ 中的 C_2 部分进行重加密：

$$C_2' = \frac{C_2}{\mathrm{UKID}} = \frac{\left(v\prod_{j \in W} \omega_{n+1-j}\right)^c}{\left(\omega_{n+1-\mathrm{ID}}\right)^c} = \frac{\left(v\prod_{j \in W} \omega_{n+1-j}\right)^c}{\left(\omega^{(f^{n+1-\mathrm{ID}})}\right)^c} \tag{15}$$

得到新的密文头：

$$\left[\widehat{\mathcal{H}}_{\mathcal{P}}\right] = \Big(\mathcal{T}, C, C_1, C_2', \Big\{\left(\overline{E}_{t_i}, E'_{t_i}\right), \left(E_{t_j}, E'_{t_j}\right), \left(E_{\mathrm{Pcode}_l}, E'_{\mathrm{Pcode}_l}\right), \left(E_{\mathrm{Ncode}_l}, E'_{\mathrm{Ncode}_l}\right)\Big\}_{A_l[t_i,t_j,\mathrm{Pcode}_l,\mathrm{Ncode}_l] \in \mathcal{T}}\Big)$$

5 安全分析

攻击模型定义了方案的安全性。若情形 1 或情形 2 发生，那么 FGUR 方案被认为是失败的。在这一节中，将证明 FGUR 方案的安全性。

存储在云中的数据文件是用会话密钥 $\mathrm{ek} = e(g^{\alpha}, \omega)^{\sigma}$ 加密的。假设加密 ek 的基于属性访问策略是 $\widehat{\mathrm{AP}} = A_l\left[t_i, t_j, \mathrm{Pcode}_l, \mathrm{Ncode}_l\right] \wedge A_x\left[t_i, t_j, \mathrm{Pcode}_x, \mathrm{Ncode}_x\right]$。如果基于属性访问权限为 $\widehat{\mathcal{L}}_1 = A_l\left[t_i, t_j, \mathrm{Pcode}_l, \mathrm{Ncode}_l\right]$ 的用户 uk_1 通过联合访问权限为 $\widehat{\mathcal{L}}_2 = A_x\left[t_i, t_j, \mathrm{Pcode}_x, \mathrm{Ncode}_x\right]$ 的用户 uk_2 能够恢复出 ek，则情形 1 中的第 1 个条件成立。FGUR 方案允许攻击者分别使用私钥 $\mathrm{SK}_{\widehat{\mathcal{L}}_1}$ 和 $\mathrm{SK}_{\widehat{\mathcal{L}}_2}$ 来恢复 $F_{t1} = e\left(g^{\tau'_{k1}}, \omega\right)^{\Delta_\sigma(A_l)}$ 和 $F_{t2} = e\left(g^{\tau'_{k2}}, \omega\right)^{\Delta_\sigma(A_x)}$。但是，为了区分不同的用户，$\tau'_{k1}, \tau'_{k2}$ 是唯一的。因此，攻击者不能利用 F_{t1}, F_{t2} 来获得 $T_1 = e\left(g^{\tau'_{k1}}, \omega\right)^{\sigma}$ 或 $T_2 = e\left(g^{\tau'_{k2}}, \omega\right)^{\sigma}$，从而不能恢复 ek。因此，情形 1 中的第 1 个条件不成立。

假设 ek 是用访问策略 $\widehat{\mathrm{AP}} = A_l\left[t_i, t_j, \mathrm{Pcode}_l, \mathrm{Ncode}_l\right]$ 加密的。当 $t_j < t_a$（或 $t_i > t_b$）时，若访问权限为 $\widehat{\mathcal{L}}_1 = A_l\left[t_a, t_b, \mathrm{Pcode}_l, \mathrm{Ncode}_l\right]$ 的用户 uk_1 能恢复出 ek，则情形 1 中的第 2 个条件成立。需要注意的是，由于 BDF 的单向性，当 $t_j < t_a$（或 $t_i > t_b$）时，uk_1 不可能从 D'_{t_a} 和 $\overline{D}'_{t_b}$ 导出 D'_{t_j} 和 $\overline{D}'_{t_j}$。因此，uk_1 不能得到 F_1 和 F_2，从而进一步恢复 ek。因此，情形 1 中的第 2 个条件不成立。

其次，设访问策略 $\widehat{\mathrm{AP}} = A_x\left[t_a, t_b, \mathrm{Pcode}_x, \mathrm{Ncode}_x\right]$。如果当 $\mathrm{Pcode}_x > \mathrm{Pcode}_l$ 或 $\mathrm{Ncode}_x > \mathrm{Ncode}_l$ 时，访问权限为 $\widehat{\mathcal{L}}_1 = A_l\left[t_a, t_b, \mathrm{Pcode}_l, \mathrm{Ncode}_l\right]$ 的用户 uk_1 能恢复 ek，则情形 1 中的第 3 个条件成立。需要注意的是，由于 CBE 中 BDF 的单向性，当 $\mathrm{Pcode}_x > \mathrm{Pcode}_l$ 时，uk_1 不能根据 $D'_{\mathrm{Pcode}l}$ 导出 $D'_{\mathrm{Pcode}x}$。同样的情况适用于 $\mathrm{Ncode}_x > \mathrm{Ncode}_l$。因此，情形 1 中的第 3 个条件不成立。

最后，当系统中某个用户被撤销访问权限，即用户 $\mathrm{ID} \notin W$ 时，若该用户仍能恢复 ek，则情形 1 中第 4 个条件成立。设 $\mathrm{ID} = n$ 的用户发生撤销，此时数据拥有者输入该用户 ID，生成更新密钥 $\mathrm{UKID} = \left(\omega_{n+1-n}\right)^c = \left(\omega^f\right)^c$，然后 CSP 运行密文更新算法，可得新的密文：$C_2' = \frac{C_2}{\mathrm{UKID}} =$

$\left(\omega^{\gamma}\prod_{\substack{j\in W\\ j\neq n}}\omega_{n+1-j}\right)^{c}$。最后该用户运行解密算法，得到

$$\mathrm{ek}_2=\frac{e\left(\omega_{\mathrm{ID}},C_2'\right)}{e\left(\prod_{\substack{j\in W\\ j\neq \mathrm{ID}}}\omega_{n+1-j+\mathrm{ID}},C_1\right)}\cdot\frac{1}{e\left(C_1,D_1\right)}$$
$$=1\neq e\left(\omega_1,\omega_n\right)^{c}\tag{16}$$

由于用户无法得出正确的 ek_2，故被撤销的用户无法再用之前的密钥计算出 ek，所以该情形不会发生。综上所述，情形 1 不会发生。

情形 2 的证明类似于情形 1。为了得到 ek，CSP 必须计算 $F_1\cdot F_2\cdot F_3\cdot F_4$ 来获得 $e\left(g^{\tau_k'},\omega\right)^{\Delta_\sigma(A_l)}$。由于 CSP 不被允许访问 PHR 系统，因此它不能获得足够的私钥。正如情形 1 中所证明的，不满足访问策略的实体不能恢复 ek。因此，情形 2 不会发生。

6　实验结果

本节通过仿真实验综合对比了 CBE 方案与 FGUR 方案的计算开销。实验环境为 Intel Core i3 2.3 GHz, 2G 内存，操作系统为 windows7。实验中，在比较范围 $[1,Z]$ 下，生成一个权限为 $[t_1,t_2]$ 的私钥，其中 $t_1\in_R[1,Z/4]$,$t_2\in_R[3Z/4,Z]$。同时，在时间条件 $t\in_R[Z/4,3Z/4]$ 下对数据进行加密。因此，可以确保 $\max(t-t_1,t_2-t)\geq Z/4$。

实验结果如图 2～图 7 所示。由于引入了属性层次和用户的即时撤销，所以，在 FGUR 方案中，Setup 和 GenKey 算法的计算开销要比 CBE 方案的更大一些。然而，两者的差距很小。如图 2 所示，当 Z 的取值范围为 7 ～ 70000 时，FGUR 方案的 Setup 算法在 $m=50$ 时的计算开销从 7.93 s 增加到 8.16 s，而 CBE 方案中 Setup 算法的计算开销从 5.32 s 增加到 5.35 s；如图 3 所示，当 Z 的取值范围为 7 ～ 70000 时，FGUR 方案的 GenKey 算法在 $m=100$ 时的计算开销从 10.05 s 增加到 10.28 s，而 CBE 方案中 GenKey 算法的计算开销从 6.12 s 增加到 6.45 s。

实验中，为了获得更好的比较结果，使用 $d=10$ 个具体属性来进行加密。如图 4 所示，与 CBE 方案相比，FGUR 方案的加密开销要小很多。例如，当 Z 的取值范围为 7 ～ 70000 时，FGUR 的 Encrypt 算法在 $m=50$ 时的计算开销从 26.41 s 增加到 26.49 s，而 CBE 方案中 Encrypt 算法的计算开销从 38.95 s 增加到 40.00 s。因此，FGUR 方案可以大大降低数据拥有者的加密开销，从而使用户获得更好的服务体验。

7　结束语

本文提出的 FGUR 方案实现了 PHR 云管理系统中的细粒度的访问控制及用户的实时撤销。通过将属性层次引入到 CBE 中，FGUR 方案能更高效地支持基于属性加密中的时间比较。同时，结合 BCP-ABE，当有用户被撤销之后，FGUR 方案无

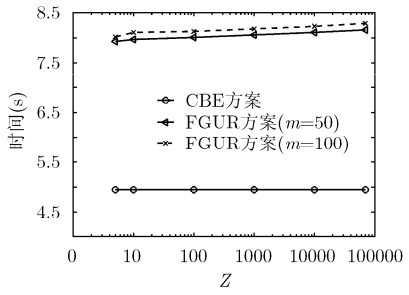


图 2　Setup 时间开销

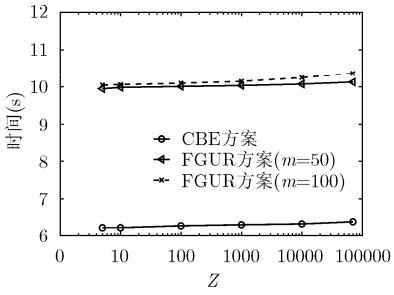


图 3　GenKey 时间开销

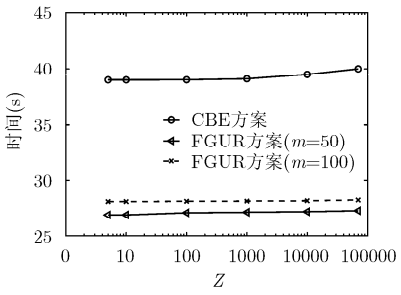


图 4　Encrypt 时间开销

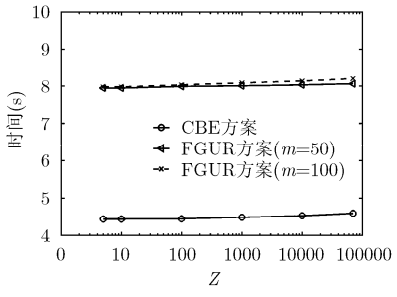


图 5　Delegate 时间开销

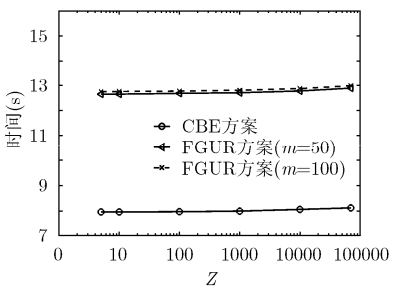


图 6　Decrypt1 时间开销

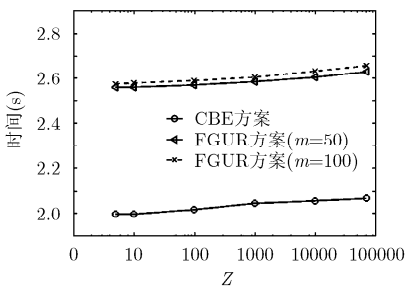


图 7　Decrypt2 时间开销

需重新分配密钥给其他未撤销用户，从而避免了系统无谓的开销。在下一步的工作中，我们将会进一步证明FGUR方案具有选择导出密钥攻击下的密钥安全(KS-CDA)和选择导出密钥攻击下的语义安全(SS-CDA)。

参 考 文 献

[1] TANG P C, ASH J S, and BATES D W. Personal health records: Definitions, benefits, and strategies for overcoming barriers to adoption[J]. *Journal of the American Medical Informatics Association*, 2006, 13(2): 121–126. doi: 10.1197/jamia.M2025.

[2] GUO L, ZHANG C, SUN J, *et al*. PAAS: A privacy-preserving attribute-based authentication system for ehealth networks[C]. Distributed Computing Systems (ICDCS), 2012 IEEE 32nd International Conference, Macau, China, 2012: 224–233.

[3] ARMBRUST M, FOX A, GRIFFITH R, *et al*. A view of cloud computing[J]. *Communications of the ACM*, 2010, 53(4): 50–58. doi: 10.1145/1721654.1721672.

[4] WANG G, LIU Q, and WU J. Hierarchical attribute-based encryption for fine-grained access control in cloud storage services[C]. Proceedings of the 17th ACM Conference on Computer and Communications Security, Chicago, USA, 2010: 735–737.

[5] BALAMURUGAN B, KRISHNA P V, KUMAR N S, *et al*. An Efficient Framework for Health System Based on Hybrid Cloud with ABE-Outsourced Decryption[M]. India: Springer India, 2015: 41–49.

[6] SANGEETHA D, VIJAYAKUMAR V, THIRUNAVUKKARASU V, *et al*. Enhanced Security of PHR System in Cloud Using Prioritized Level Based Encryption[M]. Germany: Springer Berlin Heidelberg, 2014: 57–69.

[7] YAO X, LIN Y, LIU Q, *et al*. Efficient and privacy-preserving search in multi-source personal health record clouds[C]. 2015 IEEE Symposium on Computers and Communication(ISCC), Larnaca, Cyprus, 2015: 803–808.

[8] BOLDYREVA A, CHENETTE N, and O'NEILL A. Order-preserving Encryption Revisited: Improved Security Analysis and Alternative Solutions[M]. Germany: Springer Berlin Heidelberg, 2011: 578–595.

[9] 王尚平, 余小娟, 张亚玲. 具有两个可撤销属性列表的密钥策略的属性加密方案[J]. 电子与信息学报, 2016, 38(6): 1406–1411. doi: 10.11999/JEIT150845.
WANG Shangping, YU Xiaojuan, and ZHANG Yaling. Revocable key-policy attribute-based encryption scheme with two revocation lists[J]. *Journal of Electronics & Information Technology*, 2016, 38(6): 1406–1411. doi: 10.11999/JEIT150845.

[10] 李双, 徐茂智. 基于属性的可搜索加密方案[J]. 计算机学报, 2014, 37(5): 1017–1024. doi: 10.3724/SP.J.1016.2014.01017.
LI Shuang and XU Maozhi. Attribute-based public encryption with keyword search[J]. *Chinese Journal of Computers*, 2014, 37(5): 1017–1024. doi: 10.3724/SP.J.1016.2014.01017.

[11] ZHU Y, HU H, AHN G J, *et al*. Comparison-based encryption for fine-grained access control in clouds[C]. Proceedings of the Second ACM Conference on Data and Application Security and Privacy, San Antonio, USA, 2012: 105–116.

[12] ATTRAPADUNG N and IMAI H. Conjunctive Broadcast and Attribute-based Encryption[M]. Germany: Springer Berlin Heidelberg, 2009: 248–265.

刘 琴： 女，1982 年生，助理教授，博士，研究方向为云计算、大数据和隐私保护.

刘旭辉： 男，1990 年生，硕士，研究方向为云安全.

胡柏霜： 女，1993 年生，硕士，研究方向为云安全.

张少波： 男，1979 年生，讲师，博士生，研究方向为隐私保护和云安全.