多云服务提供者环境下的一种用户密钥撤销方法

李拴保*①②③ 王雪瑞④ 傅建明①② 张焕国①②
①(武汉大学空天信息安全与可信计算教育部重点实验室 武汉 430072)
②(武汉大学计算机学院 武汉 430072)
③(河南财政税务高等专科学校 郑州 451464)
④(河南工程学院计算机学院 郑州 451191)

摘 要：密钥信息泄露是互联云服务难题之一，为解决该问题，该文提出一种基于属性环签名的用户密钥撤销方案。该方案以互联云的用户密文访问方法为研究对象，论述了无属性泄露的密文矩阵映射机制，多授权者自主扩展属性集生成密钥，从而令云服务提供者(CSP)无法获得用户完整属性，达到消除属性存储负载的目的。另外，该方案以撤销环与单调张成算法为基础设计用户签名验证撤销机制，令CSP、授权者与用户共同组成属性环，接受CSP定义密文访问结构，用户签名只有通过源CSP验证才能访问密文，授权者撤销部分属性失效用户解密密钥，从而达到权限撤销不影响其它用户访问的目的。该方案以密文策略属性基加密(CP-ABE)与单调张成算法为基础设计多用户组合属性共谋抵抗机制，用以保护属性的机密性。最后，给出该方案通信成本和计算效率的性能分析，用以验证该方法的有效性。

关键词：云计算；环签名；访问结构；验证；共谋
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1009-5896(2015)09-2225-07
DOI: 10.11999/JEIT150205

User Key Revocation Method for Multi-cloud Service Providers

Li Shuan-bao①②③ Wang Xue-rui④ Fu Jian-ming①② Zhang Huan-guo①②
①(*Key Lab of Aerospace Information Security and Trusted Computing Ministry of Education*, *Wuhan* 430072, *China*)
②(*School of Computer*, *Wuhan University*, *Wuhan* 430072, *China*)
③(*Henan College of Finance and Taxation*, *Zhengzhou* 451464, *China*)
④(*College of Computer Science and Technology of Henan Institute of Engineering*, *Zhengzhou* 451191, *China*)

Abstract: Key information leakage is one of the most serious problems in Intercloud service, to solve this problem, a scheme of user key revocation on attribute-based ring signatures is proposed. Focused on user ciphertext access in Intercloud, the mechanism of ciphertext matrixes mapping without attribute leakage is discussed, multi-authority can extend attribute sets for generation key, then full user attributes can not be acquired by Cloud Service Providers (CSP), thus overhead on attribute storage is reduced. In addition, user signature verification revocation based on revocable ring and monotone span programs is designed, which constitutes ring of CSPs, authorities and users. Receiving CSP can define ciphertext access structure, users can access ciphertext through source CSP verifying, and authorities can remove decryption key from attribute-lost users without affecting any other users. The mechanism of collusion resistance with integrating attributes on the basis of Ciphertext-Policy Attribute Base Encryption (CP-ABE) and monotone span programs is discussed, with which user attribute confidentiality can be protected from leakage. Finally, to prove the effectiviness of the proposed model, the performance analysis of communication cost and computational efficiency are verified.

Key words: Cloud computing; Ring signature; Access structure; Verify; Collusion

1 引言

云计算通过对资源、服务虚拟化整合与配置，为用户提供灵活的定制服务。互联云[1]由多个云服务提供者(Cloud Service Providers, CSP)组成，通过云之间互操作扩大计算能力和存储能力，为用户提供跨云资源租赁服务；但是互联云面临用户权限更新及信息泄露等安全威胁[2,3]。针对云环境下的用户权限更新问题，文献[4]提出了基于身份和属性的加密访问控制[5–7]实现云安全服务体系，但是没有涉及互联云的用户权限更新。特别是CSP用户密钥撤

2015-02-03收到，2015-05-18改回，2015-06-26网络优先出版
国家自然科学基金(61373168, 61202387)，教育部高等学校博士学科点专项科研基金(20120141110002)和河南省软科学研究基金(132400410165, 142400410263, 142400410267, 142400411039)资助课题
*通信作者：李拴保 phdfuli@whu.edu.cn

销会导致互联云内其它用户信息泄露，使得多CSP的数据安全具有不确定性，因此云安全联盟把云服务滥用[2]列为2013年9个重要的云安全威胁之一。

云环境用户密钥撤销，从身份基加密和属性基加密(Attribute Base Encryption, ABE)两个角度提出解决方案。面向单CSP环境，身份基加密系统通过设置用户私钥生命周期，用户只能在有效期内访问服务。在ABE系统中，授权者为用户生成私钥，数据属主利用自身属性加密数据，密文满足私钥策略解密数据；或者，数据属主利用属性树加密数据，私钥满足密文策略解密数据；当属性被更新，私钥自动失效。面向多CSP环境，文献[8]提出了一种数字身份管理框架(Digital Identity Management Framework, DIMF)，用户向注册者申请源证书，源CSP为用户提供认证证书，接受CSP响应源CSP请求为用户提供密文访问服务；注册者周期性更新证书，用户无法访问服务。

在单CSP环境下，ABE属性更新撤销用户私钥影响共享属性的其它用户访问，授权者控制属性更新，无法应用到多CSP环境。在多CSP系统中，注册者更新用户源证书，用户无法访问接受CSP服务，并且泄露用户密钥关联的隐私信息。特别在大规模用户背景下，证书更新成为用户权限更新的系统瓶颈。以DIMF为基础，源CSP控制用户匿名认证和访问，为用户提供细粒度数据服务，解决隐私泄漏难题。

云计算环境中用户密钥撤销主要有基于实体的撤销系统和基于证书的撤销系统两种方法。基于实体的撤销系统，CP-ABE(Ciphertext Policy-ABE)定义了用户访问密文的权限结构，适合云环境下的用户密钥管理。CP-ABE时间属性嵌入用户私钥[9]，周期性撤销用户密文访问权限；CP-ABE组合PRE[10,11]，撤销用户部分属性导致私钥失效，广播、CP-ABE和属性分割[12,13]组合从系统级和属性级撤销私钥，影响共享属性子集的用户访问；ABE和群签名[14]组合从属性级撤销私钥，没有定义新用户访问结构；CP-ABE和层级密钥[7,15]融合撤销用户私钥，降低了系统计算效率。基于证书的撤销系统，通过失效的代理认证撤销用户密钥。将与认证证书关联的源CSP[8]作为用户认证代理，撤销CSP服务特定属性使得用户密钥失效，攻击者根据撤销属性可以恢复整体属性，证书持续更新增加系统开销；对用户属性分类申请多个不同代理[16]，批处理撤销某类属性使密钥失效，增加额外审计开销；将属性分为多个元组，利用父类关系设置代理认证链[17]，撤销某一属性元组使得密钥失效，增加管理认证链开销；用户证书关联多个级别属性[6]，撤销级别较高属性使得证书密钥失效，需要定义与属性级别相关服务。综上所述，CP- ABE是云环境下实现用户密钥撤销与隐私信息保护的有效方式， DIMF证书管理是密钥撤销系统的一个计算瓶颈。因此，多CSP环境下保护隐私信息的用户密钥撤销方法仍是一个开放性难题。

2 预备知识

双线性映射[18]基本原理：假设$\mathbb{G}$，G_{T}分别是素数p阶的加法、乘法循环群，生成元$g\in\mathbb{G}$，双线性映射$e:\mathbb{G}\times\mathbb{G}\to G_{\mathrm{T}}$具有下列特征：双线性性：$\forall\ u,v\in\mathbb{G}$和$a,b\in Z_{\mathrm{p}}$，有$e(u^{a},v^{b})=e(u,v)^{ab}$；非退化性：$e(g,g)\neq1$；可计算性：$\forall\ p,q\in G_{\mathrm{T}}$，存在算法可计算$e(p,q)$。

假设$\mathbb{G}$是素数p阶的双线性群，在$\mathbb{G}$上的判定双线性Diffie-Hellman[18]定义如下。生成元$g\in\mathbb{G}$和指数$a,b,s\in Z_{\mathrm{p}}$。元组$(g,g^{a},g^{b},g^{s})\in\mathbb{G}^{4}$和元素$Z\in G_{\mathrm{T}}$作为输入，决定$Z=e(g,g)^{abs}$输出。如果$|P_{\mathrm{r}}[\beta(g,g^{a},g^{b},g^{s},(g,g)^{abs})=0]-P_{\mathrm{r}}[\beta(g,g^{a},g^{b},g^{s},z)=0]|\geq\varepsilon$，存在一个算法$\beta$输出$b\in\{0,1\}$，在$\mathbb{G}$上具有优势$\varepsilon$解决DBDH难题。如果没有多项式时间算法具有不可忽略优势解决DBDH难题，DBDH假设在$\mathbb{G}$上成立。

单调张成方案[19]，设$\theta:\{0,1\}^{\mathrm{n}}\to\{0,1\}$是一个单调布尔函数，域$\mathbb{F}$上的$\theta$是域$\mathbb{F}$入口的$\mathrm{l}\times\mathrm{t}$矩阵$\boldsymbol{A}$，标记函数$a:[\mathrm{l}]\to[\mathrm{n}]$关联矩阵$\boldsymbol{A}$每一行以$\theta$作为输入变量，对任意$\{x_1,x_2,\cdots,x_{\mathrm{n}}\}\in\{0,1\}^{\mathrm{n}}$，满足下式$\theta(x_1,x_2,\cdots,x_{\mathrm{n}})=1\Leftrightarrow\exists\forall v\in\mathbf{F}^{\mathrm{l}\times\mathrm{t}}:[1,0,\cdots,0]$且$(\forall i:x_{\mathrm{a(i)}})=0,\Rightarrow v_i=0$。

3 多 CSP 用户密钥撤销系统与安全模型

本文以DIMF框架为基础，授权者、用户、CSP基于属性组成环即$\mathrm{R}=\omega_{\mathrm{l}}\cup\omega_2\cup\cdots\cup\omega_{\mathrm{n}}$。在双线性映射、DBDH困难性假设和单调张成方案下，本文扩展与融合属性基环签名、撤销环、CP-ABE、高效属性签名和分布式属性基加密，构造不泄露用户隐私的用户密钥撤销方案。以密文访问方法中心，首先，引入属性基环签名[20]、多授权机制[21]生成公钥和私钥，源CSP利用解签名方法验证用户真实性，基于分布式属性基加密与单调张成算法[19]设计密文映射隐私保护方法；其次，引入撤销环签名[5]、CP-ABE[22]访问机制，撤销部分属性失效解密私钥，不影响共享属性用户访问；最后，引入高效属性签名与CP-ABE重构属性环，抵制用户共谋申请签名私钥，获得访问权限。文献[13,15]通过属性撤销与代理重加密撤销私钥，泄露部分隐私信息。在方案中，

授权者管理系统参数和属性集合，用户作为环成员向授权者申请签名私钥，用户向源CSP验证身份访问接受CSP服务。该方案包含7个算法，其基本框架如图1所示。

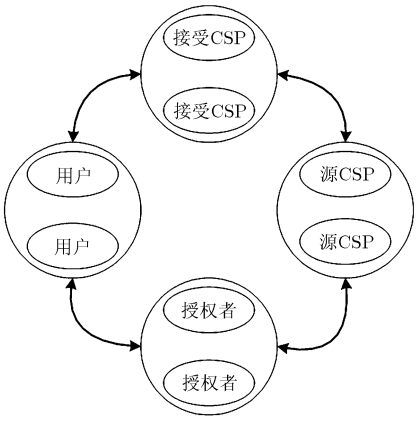

图 1 多 CSP 用户密钥撤销方案框架

多 CSP 环境下用户密钥撤销系统方案(Scheme on User Key Revocation in Multi-CSP System, SUKRMCS)基本定义如下。

定义 1　多 CSP 环境下用户密钥撤销方案是下列算法的一个元组：Setup, Encrypt, Keygen, Signature, Verify, Decrypt 和 Revoke。

初始化 Setup(λ,R)→GP,MSK,PK。算法由授权者运行，用户、授权者、源 CSP 和接受 CSP 基于属性组成环 R，输入 R 和给定安全参数λ；系统输出授权者公钥 PK 与私钥 SK、系统参数 GP 和环主密钥 MSK。

加密 Encrypt(M,R,($\boldsymbol{A}$,ρ),GP,PK)CT。算法由接受 CSP 运行，消息 M, R，访问结构($\boldsymbol{A}$,ρ), GP 和 PK 作为输入，输出云中密文 CT。

密钥生成 Keygen(R,GP,ω_{a},ω_{u},MSK) $D_{\omega_{\mathrm{u}}}$。算法由授权者运行，R, GP，授权者属性集ω_{a}，用户属性集ω_{u}和 MSK 作为输入，系统输出一个基于ω_{a},ω_{u}和 R 的用户环签名私钥$S_{\omega_{\mathrm{u}}}$。

环签名 Signature(GP, R, M,ω_{u},$\boldsymbol{A}$,S_{ω_u})$\longrightarrow\vartheta$。算法由用户运行，GP, R, M,ω_{s}, 单调张成矩阵 $\boldsymbol{A}$ 和签名私钥$S_{\omega_{\mathrm{u}}}$作为输入，系统输出用户对 M 的环签名ϑ。

环验证 Verify(R,ϑ,M,$\boldsymbol{A}$,GP) $\longrightarrow$签名ϑ是否有效。算法由源 CSP 运行，R,ϑ, M, $\boldsymbol{A}$ 和 GP 作为输入，系统输出用户签名ϑ是否有效。

解密 Decrypt(CT,GP,SK,R) $\longrightarrow$M。算法由用户运行，CT, GP, SK 和 R 作为输入，系统输出明文 M。

环撤销 Revoke(R,ω_{u},ω_{a},GP)$\longrightarrow$R′,$\omega_{\mathrm{u}}^{'}$。算法由授权者运行，R,ω_{u},ω_{a}和 GP 作为输入，系统输出新环 R′和新用户属性集$\omega_{\mathrm{u}}^{'}$。

SUKRMCS 系统安全模型假设授权者可信，CSP 不可信，给出系统 IND-SUKRMCS-CCA2 安全规则。

系统建立(Setup)：　挑战者 $\mathcal{C}$ 输入安全参数 $\boldsymbol{\lambda}$、授权者属性集ω_{a}，运行 Setup，计算 GP, MSK 和授权者密钥(PK,SK), $\mathcal{C}$ 以 GP 响应攻击者 $\mathcal{A}$。

第 1 阶段(Phase 1)：　$\mathcal{A}$ 执行多项式数量级界的自适应性密文、密钥、签名、验证、解密和撤销询问，每一次询问取决于前面已询问的结果，$\mathcal{C}$ 运行相应算法响应 $\mathcal{A}$。

加密询问(Encrypt Query)：$\mathcal{A}$ 输入 R,M,GP,($\boldsymbol{A}$,ρ)和 PK, $\mathcal{C}$ 以一个密文 CT 响应。

密钥询问(Keygen Query)：$\mathcal{A}$ 输入ω_{a},ω_{u},R 和 GP, $\mathcal{C}$ 以一个密钥$S_{\omega_{\mathrm{u}}}$响应。

签名询问(Signature Query)：$\mathcal{A}$ 输入 M,ω_{u}, R 和$S_{\omega_{\mathrm{u}}}$, $\mathcal{C}$ 以一个签名ϑ响应。

验证询问(Verify Query)：$\mathcal{A}$ 发送ϑ, M 和 GP, $\mathcal{C}$ 以逻辑数值 True 或 False 响应。

解密询问(query)：$\mathcal{A}$ 输入 R, CT 和 GP, $\mathcal{C}$ 以明文 M 响应。

撤销询问(Revoke Query)：$\mathcal{A}$ 发送ω_{u},ω_{a}, R 和 GP, $\mathcal{C}$ 以新环 R′和新用户属性集$\omega_{\mathrm{u}}^{'}$响应。

挑战阶段(Challenge)：$\mathcal{A}$ 发送两个元组(a_0,m_0,ω_{a_0},PK_{a_0},)与(a_1,m_1,ω_{a_1},PK_{a_1})随机选择一个比特 b$\in$(0,1), $\mathcal{C}$ 生成签名私钥(S_0,S_1)响应 $\mathcal{A}$。

第 2 阶段(Phase 2)：　和第 1 阶段一样。

猜测阶段(Guess)：　最后，$\mathcal{A}$ 提交一个b'。如果$b'=\mathrm{b}$，那么 $\mathcal{A}$ 在游戏中获胜。攻击者 $\mathcal{A}$ 的优势定义为 adv($\mathcal{A}$)=$|2P_{\mathrm{r}}[b'=\mathrm{b}]-1|$，其中$P_{\mathrm{r}}[b'=\mathrm{b}]$表示$b'=\mathrm{b}$的概率。

定义 2　一个多 CSP 环境下的 SUKRMCS 系统在自适应选择密文攻击下是安全的，如果任何多项式时间算法攻击者在 IND-SUKRMCS-CCA2 游戏中获胜的概率最多具备一个可忽略的优势。

4　多 CSP 用户密钥撤销方案具体构造与性能分析

4.1 具体构造

多 CSP 用户密钥撤销方案涉及 4 方实体，源 CSP、接受 CSP、用户和授权者。具体构造包括 7 个阶段：用户密钥撤销系统建立、接受 CSP 数据加密服务、授权者环签名私钥生成服务、用户签名服务、源 CSP 验证服务、用户解密服务及授权者撤销密钥服务。

4.1.1 用户密钥撤销系统建立阶段 授权者管理环系统参数、密钥生成环境的初始化，为其他服务运行提供参数准备。

第 1 步 定义含有 d 个点 $\mathrm{q}(1),\mathrm{q}(2),\cdots,\mathrm{q}(d)$ 的 $d-1$ 度多项式环上的拉格朗日插值公式 $\Delta_{j,\varphi(x)}$，对 $\forall i\in Z_{\mathrm{p}}$，假设 φ 是 Z_{p} 中的 d -元素集合；

$$\Delta_{j,\varphi(x)}=\prod\nolimits_{i\in\varphi,j\neq i}\frac{x-i}{j-i} \tag{1}$$

第 2 步 定义多项式环 R，授权者与用户、源 CSP 和接受 CSP 构造一个环 $\mathrm{R}=\omega_1\cup\omega_2\cup\cdots\cup\omega_{\mathrm{n}}$；

第 3 步 setup($\boldsymbol{\lambda}$,R)算法初始化，给定 $\boldsymbol{\lambda}$,R，系统选择 $\mathbb{G}$ 加法循环群、$\mathbb{G}_{\mathrm{T}}$ 乘法循环群，两个阶均为素数 $\mathrm{N}=p_1p_2p_3$；双线性映射 $\mathrm{e}:\mathbb{G}\times\mathbb{G}\to G_{\mathrm{T}}$，生成元 $g\in\mathbb{G}$。设 $\boldsymbol{\Omega}=\{\Omega_1,\Omega_2,\cdots,\Omega_{d-1}\}$ 一个 $d-1$ 缺省属性集合，满足拉格朗日插值公式(1)；设U是通用属性集合，且 $|\mathrm{U}|=\max$；

第 4 步 系统选择随机数 $\mathrm{w}\in Z_{\mathrm{N}}$ 和生成元 $g_1\in\mathbb{G}$，计算 $g_2=\mathrm{g}^{\mathrm{w}}$ 和 $\beta=\mathrm{e}(g_1,g_2)$；

第 5 步 定义密码学哈希函数 $H_1,H_2,(0,1)^*\to\mathbb{G}$，用于密文不可区分以及属性集到群 G_{T} 元素的映射；

第 6 步 系统选择生成元 $t_1,t_2,\cdots,t_{\max}\in\mathbb{G}$ 及随机数 $\mathrm{a},\mathrm{b},\mathrm{c},\mathrm{q}\in Z_{\mathrm{N}}$，计算 $\mathrm{C}=g^{\mathrm{c}}$，$A_0=t_0^{\mathrm{q}},A_j=t_j^{\mathrm{a}}$，$B_j=t_j^{\mathrm{b}}\ (\forall j\in[\max])$；

第 7 步 授权者属性集 ω_{a}，系统选择随机数 $\alpha_i,y_i\in Z_{\mathrm{N}}$，计算授权者公钥 $\mathrm{PK}_{\omega_{\mathrm{a}}}=\{\mathrm{e}(g_2,g_2)^{\alpha_i},g_2^{y_i}\}$、私钥 $\mathrm{SK}_{\omega_{\mathrm{a}}}=\{\alpha_i,y_i\}(\forall i)$；

第 8 步 系统发布系统参数 $\mathrm{GP}=\{\mathbb{G},g,g_1,g_2,\beta,H_1,H_2,A_0,\cdots,A_{\max},B_1,\cdots,B_{\max},\mathrm{C}\}$，保存环主密钥 $\mathrm{MSK}=(\mathrm{a},\mathrm{b},\mathrm{c},\mathrm{q})$。

4.1.2 接受CSP数据加密服务阶段 接受CSP定义密文访问结构$(\boldsymbol{A},\rho)$，$\boldsymbol{A}$是单调张成算法矩阵，ρ 为矩阵行映射到用户属性集 ω_{u}。接受CSP利用$(\boldsymbol{A},\ \rho)$，R,GP和 $\mathrm{PK}_{\omega_{\mathrm{a}}}$ 加密M输出密文CT。

第 1 步 Encrypt(R,M,$(\boldsymbol{A},\rho)$,GP,$\{\mathrm{PK}_{\omega_{\mathrm{a}}}\}$)算法初始化，$(\boldsymbol{A},\rho)$为 $n\times l$ 行列式；

第 2 步 定义多项式 $Q_{\mathrm{R}}(0)=Q_{\theta(\mathrm{n}\times\mathrm{l})}(A)$，设 d_{R} 表示 Q_{R} 的度，k_{R} 表示环内的成员数，$d_{\mathrm{R}}=k_{\mathrm{R}}-1$；

第 3 步 系统选择随机数 $\mathrm{s}\in Z_{\mathrm{N}}$ 且 $Q_{\mathrm{R}}(0)=\mathrm{s}$；选择随机矢量 $\boldsymbol{w},\mathrm{v}\in Z_{\mathrm{N}}^{\mathrm{l}}$，设 ρ 表示 $\theta\cdot\omega$ 为矩阵第 ω 行，r 表示 $\theta\cdot\mathrm{v}$ 为矩阵第 v 列。系统计算密文为

$$\mathrm{CT}_0=\mathrm{M}\,\mathrm{e}(g_2,g_2)^{\alpha_i\mathrm{s}} \tag{2}$$

$$\mathrm{CT}_1=\mathrm{e}(g_2,g_2)^{\alpha_i(\mathrm{a}+\mathrm{b}\rho)(\mathrm{c}+\mathrm{q}r)} \tag{3}$$

$$\mathrm{CT}_2=g_2^{y_iQ_\rho(0)} \tag{4}$$

$$\mathrm{CT}_3=H_1\left(g_2^{y_iQ_{\mathrm{r}}(0)}\right),\ \forall i \tag{5}$$

第 4 步 系统选择随机数 $\mathrm{f}\in Z_{\mathrm{N}}$，计算哈希值 $C'=H_2(\mathrm{R}\,\|\,\mathrm{CT}_0\,\|\,\mathrm{CT}_1\,\|\,\mathrm{CT}_2\,\|\,\mathrm{CT}_3\,\|\,\mathrm{f})H_1(\Omega\,\|\,d_{\mathrm{R}})$，输出密文 $\mathrm{CT}=\{\mathrm{R},\mathrm{CT}_0,\mathrm{CT}_1,\mathrm{CT}_2,\mathrm{CT}_3,C'\}$。

4.1.3 授权者密钥生成服务阶段 授权者为用户生成签名私钥，用于向源CSP验证真实属性，访问接受CSP的密文数据服务。

第 1 步 算法 Keygen(R,GP,ω_{a},ω_{u},MSK)初始化，系统验证 $\omega_{\mathrm{u}}\subset\mathrm{R}$ 且 $Q_{\omega_{\mathrm{u}}}(A)=0$；

第 2 步 系统选择随机数 $\mathrm{w}\in Z_{\mathrm{N}}$，选择 $d-1$ 次数多项式 Q_{R} 使得 $Q_{\mathrm{R}}(0)=\mathrm{w}$，满足拉格朗日插值公式(1)；扩展新属性集 $\hat{\omega}_{\mathrm{u}}=\omega_{\mathrm{u}}\cup\Omega$，对 $\forall\mathrm{j}\in\varphi$ 选择随机数 $\mathrm{d},\mathrm{z},r_{\mathrm{j}}\in Z_{\mathrm{N}}$，系统计算

$$d_0=g_1^{\mathrm{q}(\hat{\omega}_{\mathrm{u}})}\left(H_1(\mathrm{e}(\mathrm{g}_2,\mathrm{g}_2)^{\alpha_{\mathrm{i}}})\right)^{r_{\mathrm{j}}} \tag{6}$$

$$d_1=g_2^{y_i}\left(H_1(\mathrm{j})\right)^{r_{\mathrm{j}}} \tag{7}$$

$$\mathrm{d}=\mathrm{g}^{(\mathrm{q}+\mathrm{w})/z} \tag{8}$$

系统计算 $S_{\hat{\omega}_{\mathrm{u}}}=(\mathrm{d}\ \ d_0,d_1)\ (\forall\mathrm{i},\mathrm{j}\in\varphi)$。

第 3 步 设属性集 $\mathcal{A}\in\mathrm{R}$，选择生成元 $\mathrm{K}\leftarrow\mathbb{G}$，系统计算

$$K_0=\mathrm{d}d_0K^{1/\mathrm{c}} \tag{9}$$

$$K_{\mathrm{t}}=d_1K^{1/(\mathrm{a}+\mathrm{bt})}(\forall\mathrm{t}\in\mathcal{A}\text{且}\mathrm{t}\le\mathrm{n}) \tag{10}$$

$$K_{\omega_{\mathrm{a}},\mathrm{R},\hat{\omega}_{\mathrm{u}}}=g^{\alpha_i}\left(H_1(\omega_{\mathrm{a}},\mathrm{R},\hat{\omega}_{\mathrm{u}})\right)^{y_i} \tag{11}$$

第 4 步 设 $S_0=K_0$ 且 $S_1=K_{\omega_{\mathrm{a}},\mathrm{R},\hat{\omega}_{\mathrm{u}}}K_t$，输出用户环签名私钥 $S_{\hat{\omega}_{\mathrm{u}}}=(S_0,S_1)\ (\forall\mathrm{j}\in\hat{\omega}_{\mathrm{u}},\mathrm{t}\in\mathcal{A}\text{ 且 }\mathrm{t}\le\mathrm{n})$。

4.1.4 用户签名服务阶段 用户映射属性信息为矩阵变量，向源 CSP 认证扩展属性签名消息。

第 1 步 Signature(GP,R,M,$S_{\hat{\omega}_{\mathrm{u}}}$,$\omega_{\mathrm{u}}$,$\boldsymbol{A}$)算法初始化，源 CSP 公钥为 GP，用户和源 CSP 通过安全通道交换密钥；

第 2 步 系统选择 d 个元素 $\varepsilon_d=\{\varepsilon_1,\cdots,\varepsilon_{\mathrm{f}}\}\in\{A_{\max}\}$，选择 d 个元素 $\varepsilon_d'=\{\varepsilon_{d+1},\cdots,\varepsilon_{2d}\}\in\{B_{\max}\}$ 且 $(\{A_{\max}\}\cup\{B_{\max}\})\subseteq\Omega$；均满足 $d-1$ 度多项式 $Q_{\mathrm{R}}'(A)$ 且 $Q_{\mathrm{R}}'(0)=0$；

第 3 步 设 $\theta(\mathcal{A})=1,\mathcal{A}\in(A)^{\mathrm{l}\times\mathrm{t}},\theta:[\mathrm{l}]\to\boldsymbol{A}$；设 $\delta=H_2(\mathrm{R}\,\|\,\mathrm{M}\,\|\,\theta)$，系统计算用户属性映射为矩阵变量

$$\vartheta_i=\prod_{i=1}^{l}(\varepsilon_i)^{\mathrm{M}\theta_i}\left(\mathrm{C}g^{\delta}\right)^{\varepsilon_i},\quad\forall i\in[\mathrm{l}] \tag{12}$$

$$\vartheta_j=\prod_{j=1}^{t}(\varepsilon_j)^{\mathrm{M}\theta_j}\left(\mathrm{C}g^{\delta}\right)^{\varepsilon_j},\quad\forall j\in[\mathrm{t}] \tag{13}$$

第 4 步 随机选择 $\forall\mathrm{f}\in Z_{\mathrm{N}}$ 且 $1\le\mathrm{f}\le d$，设用户签名为 ϑ 包括 4 部分即 $\vartheta=\{\vartheta_{\mathrm{f1}},\vartheta_{\mathrm{f2}},\vartheta_{\mathrm{f3}},\mathrm{U}\}_{1\le\mathrm{f}\le d}$；系统分别计算。

$$\vartheta_{\mathrm{f1}}=\vartheta_i^{S_0}g_1^{Q_{\mathrm{R}}'(A)}H_2(\mathrm{f})^{\varepsilon_d'}\ H_1\left(\mathrm{C}g^{\delta}\right)^{\varepsilon_i},\ \forall i\in[\mathrm{l}] \tag{14}$$

$$\vartheta_{\mathrm{f2}}=\vartheta_j^{S_1}g_2^{\varepsilon_{d'}Q_{\mathrm{R}'}(A)},\ \forall j\in[\mathrm{t}] \tag{15}$$

$$\vartheta_{\mathrm{f3}}=g_1^{\varepsilon_d\varepsilon_{d'}} \tag{16}$$

$$\mathrm{U}=S_0^{\mathrm{f}} \tag{17}$$

系统输出 ϑ 并传递给源 CSP。

4.1.5 源 CSP 验证签名服务阶段　源 CSP 验证用户环签名的真实性、有效性和环内成员，源 CSP 无法获得用户的任何属性信息。

第 1 步　Verify(R,ϑ,M,$\boldsymbol{A}$,GP)算法初始化，验证消息 M 和 $\hat{\omega}_{\mathrm{u}}$ 签名 ϑ 的真实性与有效性，系统计算

$$\prod_{f=1}^{d}\left(\frac{\mathrm{e}(H_1\left(\mathrm{C}g^{\delta}\right),\vartheta_{\mathrm{f2}})}{\mathrm{e}(g_1,\vartheta_{\mathrm{f1}})\mathrm{e}(H_2(\mathrm{f}),\vartheta_{\mathrm{f3}})}\right)^{\Delta_{f\varphi(0)}}=\beta \tag{18}$$

式(18)成立，用户环签名是真实的且有效；

第 2 步　验证用户来自环内成员，系统计算

$$\mathrm{e}(\mathrm{Y},A_0)=\mathrm{e}(S_0^{\mathrm{f}},t_0^{\mathrm{q}})=\mathrm{e}(g_2,g_1)^{Q_{\mathrm{R}}(0)} \tag{19}$$

式(19)成立，用户完整属性属于环 R，环成员是真实的；

第 3 步　用户签名不是伪造的，系统计算

$$\mathrm{e}(\mathrm{Y},\mathrm{C})=\mathrm{e}(S_0^{\mathrm{f}},g^{\mathrm{c}})=\mathrm{e}(g,g_1)^{\mathrm{fc}} \tag{20}$$

式(20)成立，用户签名不是伪造的。式(18)~式(20)均成立，系统输出“True”传递给接受 CSP，用户可以访问密文服务。

4.1.6 用户解密服务阶段　用户通过源 CSP 验证，作为环内成员访问接受 CSP 密文服务，接受 CSP 无法获得用户的任何属性信息；非法用户共谋无法解密密文。

第 1 步　算法 Decrypt(CT,GP,R,SK)初始化，系统计算密文可解性

$$\frac{\mathrm{CT}_1\mathrm{e}(H_2(\mathrm{R},\mathrm{M}),\mathrm{CT}_3)}{\mathrm{e}(K^{\mathrm{Q}\rho(0)},\mathrm{CT}_2)}=\mathrm{e}(g_1,g_1)^{\omega}\,\mathrm{e}(H_2(\mathrm{R},\mathrm{M}),g_1)^{r} \tag{21}$$

式(21)成立，密文是可解密的；

第 2 步　系统选择随机数 $\mathrm{t}\in Z_{\mathrm{N}}$，$\sum_x \mathrm{t}A=(1,0,\cdots,0)$，矩阵 $\boldsymbol{A}$ 的 $\omega(1,0,\cdots,0)=\mathrm{s}$，列 $\mathrm{r}.(1,0,\cdots,0)=0$，系统计算

$$\prod_x(\mathrm{e}(g_1,g_1)^{\omega}\,\mathrm{e}(H_2(\mathrm{R},\mathrm{M}),g_1)^{r})^{\theta_x}=\mathrm{e}(g_1,g_1)^{s} \tag{22}$$

解密得明文 $\mathrm{M}=\mathrm{CT}_0/\mathrm{e}(g_1,g_1)^{s}$ 且密文不可区分；

第 3 步　系统计算

$$\mathrm{e}(\mathrm{CT}_1,S_0)\neq\mathrm{e}(g_1,g_1)^{\alpha_i s} \tag{23}$$

第 4 步　系统计算

$$\mathrm{e}(\mathrm{CT}_3,S_1)\neq\mathrm{e}(g_1,g_1)^{y_i s} \tag{24}$$

式(21)~式(24)成立，用户组合属性共谋无法解密密文。

4.1.7 授权者撤销密钥服务阶段　用户解密密文后，授权者自动撤销用户私钥，并且不泄露用户任何属性信息。

第 1 步　撤销算法 Revoke(R,ω_{s},GP)初始化。从环 R 中撤销用户 ω_{u} 部分属性，定义 ω_{u} 属性子集 ω_{u}''，且 ω_{u}'' 和 ω_{s} 属性个数满足(k,n)门限保密方案[23]；定义 R 的属性子集 R'，使得 $R'=\mathrm{R}-\omega_{\mathrm{u}}''$；

第 2 步　基于 R' 计算 $C'=H_2(R',\mathrm{CT}_0,\mathrm{CT}_1,\mathrm{CT}_2,\mathrm{CT}_3)$，基于新 C' 输出重加密密文 CT=$\{R',\mathrm{CT}_0,\mathrm{CT}_1,\mathrm{CT}_2,\mathrm{CT}_3,C',\}$；

第 3 步　系统计算 Keygen(R',GP, ω_{a},ω_{u}'',MSK)用户私钥 $D_{\omega_{\mathrm{u}}''}$，用户 ω_{u}'' 无法通过源 CSP 验证不能解密密文；

第 4 步　系统计算

$$S'=S_0^{\rho}S_1^{r}=\mathrm{e}(g_2,g_1)^{Q_{\mathrm{R}}(\theta)} \tag{25}$$

用户解密密文后，密钥被撤销得到验证。

4.2 性能分析

本文方案授权者、CSP 和用户之间通信成本来自于系统参数、密钥、签名和密文，设|N|表示 Z_{N} 元素规模，$|g|$,$|g_T|$ 表示 $\mathbb{G}$,G_{T} 元素规模，n_{u} 为用户总数，n_{r} 为属性总数，与文献[13,15]比较如表 1 所示。计算成本与 DBDH 困难性假设相关，设 H_{a} 为哈希计算，P_{a} 为双线性对计算，T 为单调张成矩阵指数计算，Exp 为群指数运算；在标准模型下，本文系统指数运算、哈希运算与密文规模成本优于文献[13]和文献[15]方案，见表 2。

计算时间实验环境，基于 AMD A6-3650 主频 2.6 Ghz Hadoop 云服务器，RedHat Linux 和 8 G 内存，利用版本号为 0.5.14 的密码库(Pairing-Based Crypt-ography)，利用对称椭圆曲线基域规模为 1024 位、植入度为 1 的 α - 曲线，并且 α - 曲线有 256 位长素数 P，明文规模为 512 kB。计算时间与环和用户数量成正比，与文献[13]和文献[15]比较结果如图 2 所示，计算时间增长率小。计算效率包括计算时间和计算成本，比较通信成本和计算效率两个方

表 1 通信成本比较

通信成本	本文方案	文献[13]方案	文献[15]方案
用户和授权者	$n_{\mathrm{r}}+\lvert g\rvert$	$\lvert g_{\mathrm{T}}\rvert+2n_{\mathrm{u}}\lvert g\rvert$	$2\lvert g_{\mathrm{T}}\rvert+n_{\mathrm{u}}\lvert g\rvert$
CSP 和授权者	$\lvert\mathrm{N}\rvert+2\lvert g\rvert$	$n_{\mathrm{u}}\lvert g\rvert+\lvert\mathrm{N}\rvert$	$\lvert\mathrm{N}\rvert\lvert g\rvert+\lvert g_{\mathrm{T}}\rvert$
用户和 CSP	$\lvert\mathrm{N}\rvert+n_{\mathrm{u}}$	$\lvert\mathrm{N}\rvert\lvert g_{\mathrm{T}}\rvert+\lvert g\rvert$	$2\lvert g_{\mathrm{T}}\rvert+n_{\mathrm{u}}\lvert\mathrm{N}\rvert$

表 2 计算成本比较

指标	本文方案	文献[13]方案	文献[15]方案
对运算	$3P_{\mathrm{a}}$	$3P_{\mathrm{a}}$	$4P_{\mathrm{a}}$
指数运算	1Exp+T	4Exp	5Exp
哈希计算	$2H_{\mathrm{a}}$	$4H_{\mathrm{a}}$	$5H_{\mathrm{a}}$
密文规模	$\lvert g_{\mathrm{T}}\rvert+\lvert g\rvert$	$\lvert g_{\mathrm{T}}\rvert+2\lvert g\rvert$	$3\lvert g_{\mathrm{T}}\rvert+2\lvert g\rvert$
模型	标准	RO	RO

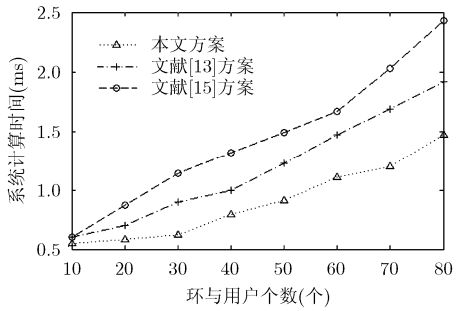

图 2 计算时间比较

面，本文系统主要在通信成本、哈希运算和密文规模优于文献[13]和文献[15]方案。

5 结束语

用户密钥撤销是多CSP服务用户权限更新焦点，DIMF是重要的身份管理基础设施。以DIMF为基础的环签名用户密钥撤销系统，通过扩展属性环签名、单调张成矩阵与多授权机制，实现扩展属性集的密钥生成与用户属性映射为矩阵策略访问树；通过融合扩展CP-ABE、单调张成矩阵、撤销环，实现无用户属性信息泄露的签名验证与密文访问，以及密文不可伪造与用户环成员真实性证明；利用单调张成矩阵与CP-ABE访问控制机制，撤销属性失效解密私钥，达到不影响共享属性用户访问；对用户和环属性重构，抵制用户签名私钥重放与共谋获得访问权限。在标准模型下，系统简化了运算规模与存储规模的复杂度，如何提高环指数运算效率需要进一步深入研究。

参 考 文 献

[1] Buyya R, Ranjan R, and Calheiros N R. InterCloud: utility-oriented federation of cloud computing environments for scaling of application services[C]. Proceedings of Algorithms and Architectures for Parallel Processing, Berlin, 2010: 13–31.

[2] Alliance C S. The notorious nine cloud computing top threats in 2013[OL]. http://cloudsecurityalliance.org/research/top threats, 2013.9.

[3] 李拴保, 傅建明, 张焕国. 环境下基于环签密的用户身份属性保护方案[J]. 通信学报，2014, 35(9): 99–111.
Li Shuan-bao, Fu Jian-ming, and Zhang Huan-guo. Scheme on user identity attribute preserving based on ring signcryption for cloud computing[J]. *Journal on Communications*, 2014, 35(9): 99–111.

[4] 冯登国, 张敏, 杨妍妍. 云计算安全研究[J]. 软件学报, 2011, 22(1): 71–83.
Feng Deng-guo, Zhang Min, and Yang Yan-yan. Study on cloud computing security[J]. *Journal of Software*, 2011, 22(1): 71–83.

[5] Liu D Y W, Liu J K, and Mu Y. Revocable ring signature[J]. *Journal of Computer Science and Technology*, 2007, 12(6): 785–794.

[6] Chuang I-hsun and Li Syuan-hao. An effective privacy protection scheme for cloud computing[C]. Proceedings of Advanced Communication Technology, Gangwon-Do, 2011: 260–265.

[7] Wang Guo-jun and Liu Qin. Hierarchical attribute-based encryption for fine-grained access control in cloud storage services[C]. Proceedings of Computer and Communications Security, Pairs, 2010: 735–737.

[8] Sherman S M C and He Yi-jun. Simple privacy-preserving identity-management for cloud environment[C]. Proceedings of Applied Cryptography and Network Necurity, Berlin, 2012: 526–543.

[9] Mao Shao-wu and Zhang Huan-guo. A resistant quantum key exchange protocol and its corresponding encryption scheme [J]. *China Communications*, 2014, 11(9): 12–23.

[10] 张倩颖, 冯登国, 赵世军. 基于可信芯片的平台身份证明方案研究[J]. 通信学报，2014, 35(8): 95–106.
Zhang Qian-ying, Feng Deng-guo, and Zhao Shi-jun. Research of platform identity attestation based on trusted chip[J]. *Journal on Communications*, 2014, 35(8): 95–106.

[11] 冯登国, 张敏, 李昊. 大数据隐私与安全保护[J]. 计算机学报, 2014, 37(1): 246–258.
Feng Den-guo, Zhang Min, and Li Hao. Big data privacy and security protection[J]. *Journal of Computer*, 2014, 37(1): 246–258.

[12] Yu Shu-cheng and Wang Cong. Achieving secure, scalable, and fine-grained data access control in cloud computing[C]. Proceedings of Computer Communications, Pairs, 2010b: 15–19.

[13] Yu Shu-cheng and Wang Cong. Attribute based data sharing with attribute revocation[C]. Proceedings of Information, Computer and Communications Security, Pairs, 2010a: 261–270.

[14] Dalia K. Attribute based group signature with revocation [OL]. http://eprint.iacr.org/2007/241.pdf, 2007.6.

[15] Wang Guo-jun and Liu Qin. Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers[J]. *Computers &Security*, 2011, 30(3): 320–331.

[16] Wei Li-fei and Zhu Hao-jin. Security and privacy for storage and computation in cloud computing[J]. *Information Sciences*, 2014, 258: 371–386.

[17] Adeela W and Asad R. A framework for preservation of cloud users' data privacy using dynamic reconstruction of metadata [J]. *Journal of Network and Computer Applications*, 2013, 36(2): 235–248.

[18] Dan B and Matt F. Identity-based encryption from the weil pairing[C]. Proceedings of Cryptology, Berlin, 2001: 213–229.

[19] Zhang Yan, Feng Deng-guo, and Zhang Zheng-feng. On the security of an efficient attribute-based signature[C]. Proceedings of Network and System Security, Berlin, 2013: 381–392.

[20] Jin Li and Kwangjo. Attribute based ring signatures[OL]. http:// eprint.iacr.org/2008/394.pdf, 2008.6.

[21] Lewko A and Waters B. Decentralizing attribute-based encryption[C]. Proceedings of EUROCRYPT, Paterson, 2011: 568–588.

[22] Bethencourt J, Sahai A, and Waters B. Ciphertext-policy attribute-based encryption[C]. Proceedings of the IEEE Security and Privacy, Paris, 2007: 321–334.

[23] Shamir A. How to share secret[J]. *Communication of Association for Computing Machinery*, 2002, 40(11): 612–613.

李拴保：　男，1972年生，博士生，副教授，研究方向为大数据、云计算、信息安全.

王雪瑞：　女，1977年生，讲师，研究方向为网络安全、云计算.

傅建明：　男，1969年生，教授，博士生导师，研究方向为网络安全、软件安全、云计算.

张焕国：　男，1945年生，教授，博士生导师，研究方向为密码学、可信计算、量子计算.