doi:10.3969/j.issn.1000-436x.2014.09.010

云环境下基于环签密的用户身份属性保护方案

李拴保[1,2,3]，傅建明[1,2]，张焕国[1,2]，陈晶[1,2]，王晶[1,2]，任必军[3]

(1.武汉大学 空天信息安全与可信计算教育部重点实验室，湖北 武汉 430072；
2.武汉大学 计算机学院，湖北 武汉 430072；3.河南财政税务高等专科学校 信息工程系，河南 郑州 451464)

摘 要：身份属性泄漏是最严重的云计算安全威胁之一，为解决该问题，提出了一种基于环签密的身份属性保护方案。该方案以云服务的数字身份管理为研究对象，论述了去中心化的用户密钥分割管理机制，用户自主选择算子在本地生成并存储密钥，从而令注册管理者(registrar)无法获得用户完全私钥，达到消除证书管理负载的目的。另外，本方案以用户访问权限为中心设计身份属性盲环签密验证机制，令用户和 CSP 组成环，基于环和自身属性用户可对消息子线性盲签密以及非交互公开密文验证，用以阻止多个 CSP 共谋导致的身份属性泄露场景，从而保护身份属性的完整性和机密性。最后，给出密文和属性强不可伪造、盲性机制的证明结果，在 DBDH 困难问题假设和适应性选择密文攻击下，方案中的用户可生成 3 个完全私钥组件，成功阻止环成员身份伪装。为验证系统有效性，围绕身份属性保护方案的综合负载问题对盲环签密算法进行性能评估，并对比同类算法以证实系统优化结果。

关键词：数字身份管理；无证书；强不可伪造性；盲性

中图分类号：TP393.08 **文献标识码**：A **文章编号**：1000-436X(2014)09-0099-13

Scheme on user identity attribute preserving based on ring signcryption for cloud computing

LI Shuan-bao[1,2,3], FU Jian-ming[1,2], ZHANG Huan-guo[1,2], CHEN Jing[1,2], WANG Jing[1,2], REN Bi-jun[3]

(1.Key Lab of Aerospace Information Security and Trusted Computing Ministry of Education, Wuhan University, Wuhan 430072, China;
2.School of Computer, Wuhan University, Wuhan 430072, China;
3.Department of Information Engineering, Henan College of Finance and Taxation, Zhengzhou 451464, China)

Abstract: Identity attribute leak as the most severe security threat of cloud computing, in order to solve this problem, a protection scheme of identity attributes based on ring signcryption was proposed. Focused on digital identity management in cloud service, which discusses user key parting management with decentralization. Users can choose some seeds for generation and storage of key, then integrated user key cannot be acquired by registrar, based on this payload on certification management is reduced. In addition, access-centric blindness ring signcryption verification for identity attribute is designed, which constitutes ring of users and CSP, combined with own attribute users can accomplish ring-oriented sub-linear blindness signcryption and non-interactive public ciphertext verifiability for messages so that integrity and confidentiality of identity attribute can be protected avoiding identity attribute leakage in collusion of multi-CSP. At last, strong blindness and unforgeability of ciphertext and attribute is proved in proposed model, three private key components can be generated by users and identity forgeability of ring member can be prevented successfully on the condition of DBDH difficult assumption and adaptive chosen-ciphertex tattacking. Effectiveness of proposed mechanism is verified via performance evaluation of blindness ring signcryption algorithm based on comprehensive payload in identity attribute protection, and optimization is confirmed compared with similar algorithms.

Key words: digital identity management; certificateless; strong unforgeability; blindness

---

收稿日期：2014-01-05；**修回日期**：2014-08-14

基金项目：国家自然科学基金资助项目(61373168, 61202387, 61272451)；教育部高等学校博士学科点专项科研基金资助项目(20120141110002)；河南省软科学计划基金资助项目(132400410723, 142400410671)

Foundation Items: The National Natural Science Foundation of China(61373168, 61202387, 61272451); The Specialized Research Fund for the Universities Doctoral Discipline Ministry of Education(20120141110002); The Soft Science Scheme of Henan Province (132400410723, 142400410671)

1 引言

云计算[1]作为一种新型计算模式，通过网络对可访问的计算资源、网络资源、存储资源、应用资源虚拟化整合和动态配置，为用户提供灵活的业务需求和 SaaS、PaaS、IaaS 计算服务，在智慧城市[2,3]等领域有着广泛应用。云服务提供资源的同时，也面临着用户身份属性泄漏的安全威胁，文献[4~8]提出了基于属性的加密访问控制方法构建云计算安全服务体系[9,10]防范针对身份属性安全的网络攻击。但是，机构用户的多样性[11~13]使属性安全防范具有更多的不确定性，因此云安全联盟仍然把用户身份安全[14]列为 2013 年 9 个重要的云安全威胁之一。针对云环境中的用户身份安全问题，现有方案主要从 2 个角度考虑，一方面是身份管理基础设施(IdM, identity management infrastructure)，另一方面是扩展数字身份管理系统(DIM, extended digital identity management system)框架，并且这些方案仅对认证用户提供服务。

面向异构云环境，IdM 利用 IDP/SP 模型提出了一个可扩展的动态云单点登录认证框架，设计了云之间身份认证方案。基于云联合服务环境，DIM 提出了一个 SPICE 系统框架（如图 1 所示），用户向 IdP 申请身份，注册者依据 IdP 身份为用户颁发证书。用户基于证书组签名向源 CSP（source CSP）验证身份，访问多个接收 CSP（receiving CSP）提供的联合服务；源 CSP 充当用户接口的作用，接收 CSP 为用户提供透明的数据存储和应用服务；此外，SPICE 组签名可以实现无关联和代理认证服务，比 IdM 有更丰富和详细的安全属性。

在 IdM 系统中，主云和外部云与 IdP 建立信任关系，主云作为断言方可以为 IdP 创建账户；如果主云通过外部云资源完成身份验证，利用 SAML 模型与所有外部云验证自身身份，需要维护内部资源和外部资源之间的负载平衡，并且 IdM 系统没有定义属性安全。在 SPICE 系统中，注册者需要存储一组签名，每个签名都是用户属性的承诺；用户通过注册者签名获得源证书，源 CSP 确信接收 CSP 期望的属性为用户颁发认证证书；攻击者不能链接同一用户重随机化的注册者签名，因此不能泄漏用户隐私；但是 SPICE 系统证书泄漏了与接收 CSP 无直接关联的部分属性，缺乏整体属性的安全保护。构造面向用户整体属性的保护系统，是本文研究云环境下身份属性保护的难点。以 SPICE 框架为基础，所有认证用户以匿名方式提交完整属性获得接收 CSP 的访问权限；与 SPICE 系统不同，以用户为中心无需 IdP 提供身份服务。

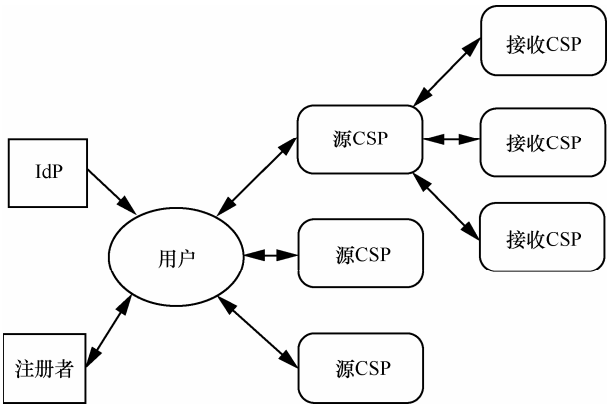

图 1 SPICE 框架

1.1 相关工作

从 IdM 和 DIM 的角度，云环境中身份安全问题逐步演变为 2 个方向：基于实体的认证系统和基于证书的认证系统。

零知识已广泛应用于基于实体认证系统的匿名身份验证。零知识证明首次应用于云计算身份认证[15]，并且设计了一种用户承诺属性合法签名执行零知识证明协议向 CSP 证明身份的方案。鉴别者利用零知识证明认证用户匿名身份而不泄漏身份标识[16]，然而 IdM 与 IdP 之间产生巨额的通信开销。个体属性集分布在多个第三方可信服务器保护用户身份隐私[17]，离散的属性部署方法不利于整体属性机密性和通信负载的降低。主云与外部云依托第三方的信任合作[18]，主云用户执行单点登录可以获得外部云所提供的资源。由于公共云的不可信，无可信第三方加密数据预测利用与多方计算协商云服务的身份管理[19]，但是无法有效扩展用户规模。面向私有云环境，基于用户身份与交互认证历史的同步保护数据隐私和身份匿名的组签名[20]，该方案仅限于小规模用户。为了同时满足身份与隐私保护，基于安全和隐私融合结构化的云服务架构[21]，该方案支持身份理解和安全隐私限制，需要模型语言组合云服务提供。

组签名已广泛应用于基于证书认证系统的密码匿名证书。将身份隐私泄漏分为存在泄漏和关联泄漏[22]，存在泄漏是用户可以鉴别的属性泄

漏，关联泄漏是用户在申请云服务时的敏感属性泄漏。基于 2 种泄漏提出了一种基于 QI-属性的不分割属性集的模糊组签名方案，产生了密文数据泄漏。文献[23]将用户隐私分为多个级别，依据级别选择合适的数据份额和组签名算法，同步实现用户身份安全和系统性能优化，但没有定义与隐私级别关联的云计算服务类型。文献[24]将与源证书关联的多个属性分为 3 种类型，个人敏感信息不做特殊处理，与 CSP 服务关联特定属性采用异构命名，与特定服务无关属性组签名隐藏处理；然而，第一类属性没有限制最少数量，攻击者可以恢复用户整体属性；属性分类和更新增加了计算开销，证书负载增加了通信开销。总之，注册者作为组管理员成为云安全服务的性能瓶颈，并且 SPICE 系统缺乏用户身份整体属性的安全机制。针对云用户身份欺骗，利用指定验证签名、批处理验证和概率样本方法[25]设计了云存储与云计算审计协议以保护用户隐私，批处理方法增加了巨额的计算开销。基于私有云用户身份敏感属性分类，将属性分割为多个元数据[26]，依据元数据的父类关系重构密码保护操作，阻止攻击者非授权访问用户数据；同时，重构密码操作支持不同签名机制，元数据关系重构与多签名机制降低了系统整体性能。

综上所述，扩展 DIM 系统满足面向身份管理的安全属性，用户一次注册认证，可以访问所有其他云服务；SPICE 框架最大优势是接收 CSP 和源 CSP 联合为用户提供服务，提高了资源利用效率，降低了服务成本。但是，SPICE 组管理员机制成为系统性能瓶颈，证书发布存在组成员伪造密文假冒签名者获得合法的认证身份。因此，基于 SPICE 框架保护用户身份整体属性安全仍是一个开放性难题。本文专注于云计算服务的最困难问题用户身份整体属性匿名保护。

1.2　主要贡献

以 SPICE 框架为基础，面向云环境的身份安全系统来源于扩展基于属性环签密[27]和无证书签密[28]方案，并且融合盲环签名[29]和强不可伪造签密[30]的属性保护机制；用户自定义签密属性，环签密允许用户代表环利用一组属性签密消息并且保护个人敏感属性，其他成员确信签密者来自环内，但不能鉴别其真实身份。文献[24, 25]以注册者为中心，通过群签名的 CA 证书与代理认证，隐藏用户身份。本文以用户访问权限为中心，利用密钥分割、盲环签名与强不可伪造签密，保护用户身份属性。首先，引入无证书签密与强不可伪造签密的密钥分割方法，用户自主选择算子生成公钥和完全私钥，CSP 服务利用解签密方法验证用户身份的真实性；其次，引入盲环签名的子线性规模方法，用户与 CSP 组成环，隐藏用户身份属性，抵制 CSP 共谋获取用户身份属性信息；最后，引入强不可伪造签密的无需直接交互的公开密文验证方法，用户生成 3 个完全私钥组件，2 个用于签密，一个用于验证，抵制环成员身份伪装。

2　准备知识

2.1　双线性映射

本文方案是基于双线性映射及双线性映射群[31]，其基本原理：假设 G 和 G_T 是素数 p 阶的加法、乘法循环群，g 是 G 的生成元，e:$G\times G\rightarrow G_T$ 是一个双线性映射。

双线性映射 e 有如下基本属性。双线性性：对任意的 $u, v\in G$ 和 $a, b\in Z$，总有 $e(u^a, v^b)=e(u, v)^{ab}$；非退化性：$e(g, g)\neq 1$；可计算性：任取 p、$q\in G_T$，存在有效算法计算 $e(p, q)$。

2.2　计算性假设

1) 计算性 Diffie-Hellman 问题

假设 G 是素数 p 阶的双线性群，在 G 上的计算性 Diffie-Hellman[31]定义。选择 G 的随机生成器 g 和随机指数 $a, b\in Z_P$，如果给定一个元组$(g, g^a, g^b)\in G^3$，在 G 上 CDH 困难性问题是计算 g^{ab}。在 G 上解决 CDH 问题，任何多项式概率时间算法 β 的优势是 $\mathrm{Adv}_{\beta}^{\mathrm{CDH}}=\Pr[\beta[g, g^a, g^b]=g^{ab}|a, b\in Z_P]$，CDH 假设是对任何概率多项式时间算法$\beta$，优势 $\mathrm{Adv}_{\beta}^{\mathrm{CDH}}$ 可以忽略不计。

2) 判定双线性 Diffie-Hellman 问题

假设 G 是素数 p 阶的双线性群，在 G 上的判定双线性 Diffie-Hellman[31]定义如下。选择 G 的随机生成器 g 和随机指数 $a, b, s\in Z_P$。如果给定一个元组$(g, g^a, g^b, g^s)\in G^4$ 和一个元素 $Z\in G_T$ 作为输入，决定 $Z=e(g, g)^{abs}$ 的输出。如果$|\Pr[\beta(g, g^a, g^b, g^s, e(g, g)^{abs})=0]-\Pr[\beta(g, g^a, g^b, g^s, z)=0]|\geqslant\varepsilon$，存在一个算法 β 输出 $b\in\{0, 1\}$，在 G 上具有优势 ε 解决 DBDH 难题。如果没有多项式时间算法具有不可忽略的优势解决 DBDH 难题，可以说 DBDH 假设在 G 上成立。

3 基于环签密的身份属性保护系统与安全模型

3.1 系统模型

以 SPICE 框架为基础的用户身份属性保护系统，通过扩展基于属性环签密系统[27]和无证书签密系统[28]，在双线性映射、DBDH 困难性假设标准模型下，融合盲环签名的子线性规模属性保护[29]和强不可伪造签密的发送双方无需交互的公开密文验证机制[30]；构造面向用户属性的去中心化盲环签密系统，保护用户身份属性安全。

以 SPICE 框架为基础的去中心化盲环签密方案，环 $C1$ 由用户和源 CSP 的属性组成，即 $C1=\omega_1 \cup \omega_2 \cup \cdots \cup \omega_N$，包括三方实体：PKG(注册者)、用户和源 CSP，PKG 负责通用属性集 U 管理、系统公共参数 *params* 和主密钥 *MSK* 生成与发布。用户依据自身属性 ω 向 PKG 申请注册和密钥生成，PKG 验证 $\omega \subset U$ 生成部分私钥通过安全通道发送给用户。用户根据部分私钥和自主秘密值，生成公钥和完全私钥；用户利用盲环签密方法向源 CSP 认证身份。环 $C2$ 由源 CSP 和接收 CSP 组成，源 CSP 通过解签密方法验证用户身份，通过源 CSP 验证的用户获得多个源 CSP 和接收 CSP 联合提供的应用服务。盲环签密身份属性保护方案框架如图 2 所示。

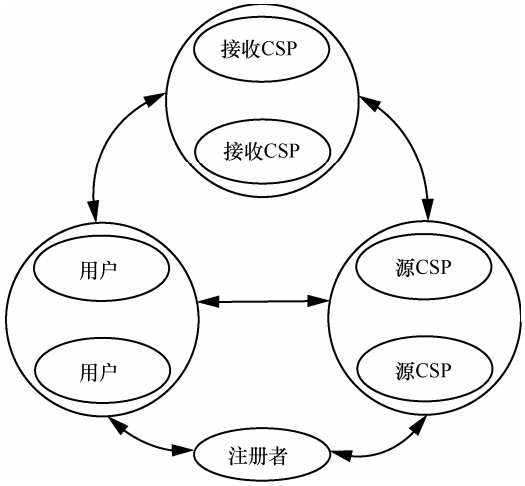

图 2 盲环签密身份属性保护方案框架

方案包含 6 个算法（见 3.2 节），算法 1）和算法 2）由 PKG 运行，算法 3）~算法 5）由用户运行，算法 6）由源 CSP 运行。为了清晰地理解算法，用表 1 中记号表示在算法中的真实含义。

表 1 盲环签密身份属性保护方案记号与含义

记号	含义	记号	含义
PKG	公共参数和密钥生成器	$SK_{\omega s}$	用户私钥
m	消息	$SK_{\omega R}$	CSP 私钥
ω_s	用户属性集	$PK_{\omega s}$	用户公钥
ω_R	CSP 属性集	$PK_{\omega R}$	CSP 公钥
$C1$	环	CT	签密文

3.2 基于环签密的用户身份属性保护框架

基于环签密的用户身份属性保护方案（SUIAPRS, scheme on user id- entity attribute protection based on ring signcryption）框架定义如下。

定义 1 盲环签密身份属性保护方案是下列算法的一个元组：setup、extract-partial-private-key、centerless-generate-user-key、extract-private-key、blind-signcryption 和 unsigncryption。其中，extract-private-key 和 blind-signcryption 用于属性保护。

1) 初始化算法 setup(k)：算法由 PKG 运行，给定安全参数 k，PKG 选择随机数 α，作为输入；算法输出主密钥 *MSK* 和公共参数 *params*，PKG 保存 *MSK* 作为秘密值。用户和源 CSP 基于身份属性组成环 $C1=\omega_1 \cup \omega_2 \cup \cdots \cup \omega_N$。

2) 部分私钥生成算法 extract-partial-private-key(*MSK*, *params*, ω_S)：算法由 PKG 运行，输入 *MSK*、*params*、用户属性集 ω_s，输出基于属性集 ω_s 的部分私钥 $D_{\omega s}$。通过安全通道，PKG 发送 $D_{\omega s}$ 给具有属性集 ω_s 的用户。

3) 公钥生成算法 centerless-generate-user-key (*params*, ω_S)：算法由具有属性集 ω_s 的用户运行，输入 *params*、属性集 ω_s，用户随机选择秘密值 $\rho_{\omega s}$，输出属性集 ω_s 的相应公钥 $PK_{\omega s}$，本地保存。用户无需证书发布公钥 $PK_{\omega s}$。

4) 完全私钥生成算法 extract-private-key (*params*, $D_{\omega s}$, $\rho_{\omega s}$)：算法由具有属性集 ω_s 的用户运行，输入 *params*、部分私钥 $D_{\omega s}$ 和秘密值 $\rho_{\omega s}$，输出具有 3 个组件的完全私钥 $SK_{\omega s}$，本地保存。

5) 盲环签密算法 blind-signcryption($C1$, m, ω_s, $SK_{\omega s}$, ω_R)：算法由具有属性集 ω_s 的用户运行，输入消息 m、环 $C1$、用户 ω_s、$SK_{\omega s}$ 和源 CSP 的 ω_R，输出签密文 CT。

6) 解签密算法 unsigncryption($C1$, CT, $SK_{\omega R}$)：算法由具有属性集 ω_R 的源 CSP 运行，输入签密文

CT、环 $C1$ 和源 CSP 完全私钥 $SK_{\omega R}$，源 CSP 验证密文 CT。如果验证 CT 有效，签密者是 $C1$ 成员，输出“Valid”；否则输出“Invalid”。

3.3 安全模型

在盲环签密身份属性保护系统，本文假设：1) 对于没有访问权限的用户，源 CSP 服务器允许认证访问；2) 源 CSP 是不可信的，服务器会尽可能获得用户的身份属性；3) 用户是不可信的，身份伪装和共谋伪造密文获得访问权限。在阐述系统安全模型前先给出 IND-SUIAPRS-CCA2 游戏规则，规则描述如下。

系统建立（setup） 挑战者 C 输入一个安全参数 k 和一个随机数 α，运行初始化算法 setup，得到系统参数 *params* 和主私钥 *MSK*。C 公开参数 *params* 发送给攻击者 A，C 秘密保存主私钥 *MSK*。

第一阶段（Phase 1）：A 执行多项式数量级界的以下询问。这些询问是以适应性的方式进行，每一次询问取决于前面已询问的结果。

1) 部分私钥提取询问(partial-private-key extract query)：A 输入属性集 ω、系统参数 *params* 和主私钥 *MSK*，得到部分私钥 D_ω=extract-partial-private-key(*MSK*, *params*, ω)。

2) 公钥提取询问(generate-user-key extract query)：A 输入系统参数 *params*、属性集 ω 和随机秘密值 ρ_ω，得到公钥 PK_ω=centerless-generate-user-key(*params*, ω, ρ_ω)。

3) 完全私钥提取询问(private-key extract query)：A 输入系统参数 *params*、部分私钥 D_ω 和秘密值 ρ_ω，得到完全私钥 SK_ω=extract-private-key (*params*, D_ω, ρ_ω)。

4) 盲环签密询问(blind-signcryption query)：A 输入 2 个属性集 ω_i、ω_j 和一个明文消息 m。C 通过计算 $D\omega_i$=extract-partial-private-key(*MSK*, *params*, ω_i)、$PK_{\omega i}$= centerless-generate- user-key(*params*, ω_i, $\rho_{\omega i}$)、$SK_{\omega i}$=extract-private-key(*params*, $D\omega_i$, $\rho_{\omega i}$)和 CT=blind-signcryption($C1$, m, ω_i, $SK_{\omega i}$, ω_j)，并将 CT 发送给 A。

5) 解签密询问(unsigncryption query)：A 输入属性集 ω_j、签密文 CT。C 通过计算 extract-partial-private-key(*MSK*, *params*, ω_j)、certificateless- generate-user-key(*params*, ω_j, $\rho_{\omega j}$)和 extract-private-key (*params*, $D_{\omega j}$, $\rho_{\omega j}$)获得 SK_j，并将 unsigncryption ($C1$, CT, SK_j)计算结果发送给 A。

挑战阶段（challenge）：A 选择挑战的 2 个明文 m_0、m_1 和 2 个属性集 ω_A、ω_B，并且 A 不能在第一阶段询问 ω_B 所对应的私钥。C 随机选择一个 b，计算 CT^*=blind-signcryption ($C1$, m_b, ω_A, $SK_{\omega A}$, ω_B)。

第二阶段（Phase 2）和第一阶段一样，A 再次适应性地执行多项式数量级的询问，并且不允许询问 ω_B 对应的私钥或以 ω_B 的名义对 CT^* 解签密询问。

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

定义 2 一个基于环签密的身份属性保护方案（SUIAPRS）在自适应选择密文攻击下是安全的，如果所有的多项式时间算法攻击者在 IND-SUIAPRS-CCA2 游戏中获胜的概率最多具备一个可忽略的优势。

4 SUIAPRS 方案具体构造、安全分析与性能分析

4.1 具体构造

在标准模型下，身份属性保护方案涉及三方：PKG、用户和源 CSP，来自于扩展与重构方案[27, 28]以及融合方案[29,30]。PKG 管理通用属性集、生成公共参数与主密钥；用户自定义属性集并向 PKG 申请密钥生成因子，PKG 根据属性生成部分私钥；用户和源 CSP 构成环，源 CSP 验证用户身份并为其提供服务。方案具体构造包括 5 个阶段：身份属性保护系统建立阶段、PKG 部分私钥提取服务阶段、用户公钥与完全私钥服务阶段、用户盲环签密阶段和源 CSP 解签密验证阶段，如下所述。

4.1.1 身份属性保护系统建立阶段

云环境下基于环签密的身份属性保护系统，PKG 负责系统参数、密钥生成环境的初始化，为用户访问云服务提供身份认证准备。

第 1 步 定义多项式环上的拉格朗日插值公式 $\Delta_{i,\,s}$，用于密钥分散管理；对任意 $i\in Z_p$，假设 S 是 Z_p 中的 d-元素集合。

$$\Delta_{i,\,s(x)}=\prod_{j\in s,\,j\neq i}\frac{x-i}{i-j} \tag{1}$$

第 2 步 定义多项式环，基于用户和源 CSP 的属性构造一个环 $C1=\omega_1\cup\omega_2\cup\cdots\cup\omega_N$。

第 3 步 setup(k)算法初始化，给定安全参数 k，PKG 选择 G、$\tilde{G}$ 加法循环群，G_T 乘法循环群，2 个阶均为素数 p；双线性映射 $e: G \times \to G_T$，g 是 G 的一个生成元。假设 U 是通用属性的集合，且$|U|=T$；$\Omega=\{\Omega_1,\cdots,\Omega_{d-1}\}$是一个 d–1 缺省属性集合，满足拉格朗日插值式(1)。

第 4 步 计算系统参数和主密钥，PKG 选择随机数 $t_1,\cdots, t_L \in Z_p$，假设 $T_i=g^{t_i}$ (i=1, …, L)；随机选择 $h_1, h_2, g_2 \in G$，选择随机数 $\alpha \in Z_p$，计算 $Y=e(g, g)^{\alpha}$，$g_1=g^{\alpha}$。

第 5 步 定义密码学散列函数 H:{0, 1}*→{0, 1}$^{|n|}$，$|n|$表示签密文的长度，用于抵制 CSP 之间共谋。

第 6 步 PKG 发布公共系统参数 $params$={G, G_T, e, g, g_1, g_2, h_1, h_2, Y, H, $\{T_i\}_{i=1}^{L}$, $\tilde{G}$ }，保存主密钥 MSK={α, g_2^{α}, h_2^{α}, $\{t_i\}_{i=1}^{L}$}。

4.1.2 PKG 部分私钥提取服务阶段

PKG 为用户生成部分私钥，用户利用部分私钥生成完全私钥，用于向源 CSP 签密消息与身份认证，访问接收 CSP 提供的应用服务。

第 1 步 用户自主定义属性集 ω_s，通过安全通道向 PKG 发送 ω_s，申请其部分私钥。

第 2 步 extract-partial-private-key(MSK, $params$, ω_s)算法初始化；PKG 验证 $\omega_s \subset U$，随机选择 d–1 次数多项式 $q(x)$使得 $q(0)=\alpha$；调用假设 $\hat{\omega}_s=\omega_s \cup \Omega$，对任意 $i, j \in \hat{\omega}_s$，计算 $D_i=g^{\frac{q(i)}{t_i}}$ 和 $D_j=g^{\frac{q(j)}{t_j}}$。

第 3 步 PKG 选择随机数 $r \in Z_p$，具有属性集 ω_s 的用户部分私钥为

$$D_{\omega_s}=(D_{\omega_s,1}, D_{\omega_s,2}, D_{\omega_s,0})$$

$$=(g_2^{\alpha}(D_i)^r, (h_2)^{\alpha}(D_j)^r, g^r)$$

$$=(g_2^{\alpha}(\prod\nolimits_{i\in\omega_s} g^{\frac{q(i)}{t_i}})^r, (h_2)^{\alpha}(\prod\nolimits_{j\in\omega_s} g^{\frac{q(j)}{t_j}})^r, g^r)$$

将结果通过安全通道发送给用户。

4.1.3 用户公钥与完全私钥服务阶段

第 1 步 用户基于 ω_s 和公共系统参数 $params$ 生成自身公钥，centerless-generate-user-key($params$, ω_s)算法初始化。

第 2 步 用户选择随机数 $\rho_{\omega} \in Z_p$ 作为秘密值，计算其基于 ω_s 的公钥 $PK_{\omega s}=e(g_1, g_2)^{\rho_{\omega R}}$，保存本地，无需证书发布。

第 3 步 extract-private-key($params$, $D_{\omega s}$, $\rho_{\omega s}$)算法初始化，用户选择随机数 $r' \in Z_p$，计算其基于 ω_s 的完全私钥

$$SK_{\omega_s}=(SK_{\omega_s,1}, SK_{\omega_s,2}, SK_{\omega_s,0})$$

$$=(D_{\omega_s,1}^{\rho_{\omega_s}}(D_i)^{r'}, D_{\omega_s,2}^{\rho_{\omega_s}}(D_j)^{r'}, D_{\omega_s,0}^{\rho_{\omega_s}}g^{r'})$$

$$=(D_{\omega_s,1}^{\rho_{\omega_s}}\left(\prod\nolimits_{i\in\omega_s} g^{\frac{q(i)}{t_i}}\right)^{r'}, D_{\omega_s,2}^{\rho_{\omega_s}}\left(\prod\nolimits_{j\in\omega_s} g^{\frac{q(j)}{t_j}}\right)^{r'}, D_{\omega_s,0}^{\rho_{\omega_s}}g^{r'})$$

$$=(g_2^{\alpha\rho_{\omega_s}}\left(\prod\nolimits_{i\in\omega_s} g^{\frac{q(i)}{t_i}}\right)^{t}, h_2^{\alpha\rho_{\omega_s}}\left(\prod\nolimits_{j\in\omega_s} g^{\frac{q(j)}{t_j}}\right)^{t}, g^t)$$

其中，$t=r\rho_{\omega_s}+r'$，$SK_{\omega_s,0}$ 和 $SK_{\omega_s,1}$ 用于盲签密消息，$SK_{\omega_s,2}$ 用于验证。

4.1.4 用户盲环签密阶段

用户向源 CSP 认证身份，获得访问源 CSP 和接收 CSP 联合提供的应用服务。用户向源 CSP 发送盲签密消息，源 CSP 验证消息来自环 $C1$ 的真实用户，证明密文是有效的，密文和属性强不可伪造。

第 1 步 blind-signcryption($C1$, m, ω_s, $SK_{\omega s}$, ω_R)算法初始化，源 CSP 公钥为 $PK_{\omega R}=e(g_1, g_2)^{\rho_{\omega R}}$，用户和源 CSP 通过安全通道相互交换公钥。

第 2 步 用户选择具有 d 个元素的属性子集 $\omega_s' \subset \omega_s$，其中属性$\{i_1,\cdots, i_f\} \in \omega_s$ 用于签密消息，属性$\{i_{f+1},\cdots, i_d\} \in \Omega$。选择消息$(m, \tilde{m}) \in G \times G$，随机数 $r'' \in Z_p$，设 $s=H(C1, m, \tilde{m}, r'')$，$S=G^s$，$\tilde{S}=\tilde{G}^s$，$X=Y^s=e(g, g)^{\alpha s}$；选择 $i \in \omega_s'$ 和 $j \in \omega_s$，计算 $E_i=T_i^s$ 和 $E_j=T_j^s$。

第 3 步 用户随机选择 Ω、Σ、$\Gamma \in Z_p$，计算 $\Sigma=((m, \tilde{G})=(G, \tilde{m}))\wedge(e(S, \tilde{G})=e(\tilde{S}, G))\wedge((Y, \tilde{S})\cdot(m, \tilde{G})=(X, \tilde{G}))$，$\Gamma=H(C1, m, \tilde{m}, S, \tilde{S})$，设 $\Omega=\{\Sigma, \Gamma\}$。

第 4 步 设 $\omega_s'=\{1, \cdots, d\}$，选择随机数 $k \in \omega_s'$，环 $C1$ 长度为 L；选择随机数 $U_L \in Z_p$，计算 $h_L=H(\Omega, X, C1, U_L, L)$；选择随机数 $r_k \in Z_p$，计算(Ω, X)散列值

$$U_k=E_k^{r_k}/\prod\nolimits_{L\in C1} U_L g^{t_L h_l s}$$

$$=g^{t_k r_k s}/\prod\nolimits_{L\in C1} U_L g^{t_L h_l s}$$

$h_k=H(\Omega, X, C1, U_K, m, k)$，$V=E_k^{h_k+r_k}$。

第 5 步 选择随机数 r'''，计算盲签密文组件

$CT_1=g^{r'''}$，$CT_2=e(g_1,h_2)^{\rho_{\omega_R} r''} \oplus (V\ PK_{\omega_R}{}^{r'''})$，$CT_3=\left(\prod_{i\in\omega_s} g^{\frac{q(i)}{t_i}}\right)^{r'''}$。

设 $CT_4=SK_{\omega_s,0}$，$m'=H(CT_1, CT_2, CT_3, CT_4, \omega_R, PK_{\omega_R})\in(0,1)^{m'}$，$m'[j]$表示 m'的第 j 位，$\pi=\{j|m'[j]=1, j=1, \cdots, m'\}$；计算 $CT_5=SK_{\omega_s,1}\left(h_1\prod_{j\in\pi} g^{\frac{q(j)}{t_j}}\right)^{r'''}$，设 $m''=(CT_1, CT_2, CT_3, CT_4, CT_5)$。

第 6 步　设 $W=(C1 /\!/ m'' /\!/ r'' /\!/ U_L /\!/ r''')\oplus H(\Omega, X, S, \tilde{S})$，盲签密文为 $CT=(C1, \Omega, W, \{U_k\}_{k=1}^{\mathbb{L}}, \{E_i\}_{i=1}^{d}, \{E_j\}_{j=1}^{L-d})$，将结果通过安全通道发送给源 CSP。

4.1.5　源 CSP 解签密验证阶段

第 1 步　验证密文有效性，用户身份属性的真实性，来自环 $C1$ 成员；Unsigncryption($C1$, CT, SK_{ω_R})算法初始化，源 CSP 向 PKG 申请部分私钥，生成公钥和完全私钥。源 CSP 公钥为 $PK_{\omega_R}=e(g_1,g_2)^{\rho_{\omega_R}}$，完全私钥为

$$SK_{\omega_R}=(SK_{\omega_R,1}, SK_{\omega_R,2}, SK_{\omega_R,0})$$

$$=\left(g_2^{\alpha\rho_{\omega_R}}\left(\prod_{i\in\omega_R} g^{\frac{q(i)}{t_i}}\right)^{t}, h_2^{\alpha\rho_{\omega_R}}\left(\prod_{j\in\omega_R} g^{\frac{q(j)}{t_j}}\right)^{t}, g^{t}\right)$$

第 2 步　源 CSP 选择具有 d 个元素的属性子集 $\omega_R'\subset\omega_R$ 和 $\omega_R'\subset\Omega$，完成下列计算和验证。

验证

$$e(h_2,g_1)^{\rho_{\omega_R} r''}=e(SK_{\omega_R,2},CT_1)/e(SK_{\omega_R,0},CT_3) \tag{2}$$

$$e(CT_5,g)=PK_{\omega_S}\ e(CT_4,\ \prod_{i\in\omega_s} g^{\frac{q(i)}{t_i}})e(CT_1,\ h_1\prod_{j\in\omega_R} g^{\frac{q(j)}{t_j}}) \tag{3}$$

$$V=CT_2 e(CT_3,\ SK_{\omega_R,2})/e(CT_1, SK_{\omega_R,1}) \tag{4}$$

式(2)~式(4)是否成立。

若式(2)~式(4)均成立，证明 CT 是有效的，且 CT 和用户属性强不可伪造。

计算

$$X'=\prod_{i\in\omega_R''} e(D_i,E_i)^{\frac{\triangle_{i,s(0)}}{2}}\prod_{j\in\omega_R'} e(D_j,E_j)^{\frac{\triangle_{j,s(0)}}{2}}$$

$$=\prod_{i\in\omega_R''} e\left(g^{\frac{q(i)}{t_i}}, g^{t_i\cdot s}\right)^{\frac{\triangle_{i,s(0)}}{2}}\prod_{j\in\omega_R'} e\left(g^{\frac{q(j)}{t_j}}, g^{t_j\cdot s}\right)^{\frac{\triangle_{j,s(0)}}{2}}$$

$$=e(g,g)^{\alpha s}$$

设 $V'=(C1 /\!/ m'' /\!/ r'' /\!/ U_L /\!/ r''')\oplus H(x'), s'=H(m'', r'')$，验证

$$U=g^{s'} \tag{5}$$

是否成立。

计算 for k=1 to L，$h_L=H(\Omega, X, C1, U_L, m, L)$，验证

$$e(g,\ \prod_{k=1}^{L} U_l\ g^{t_l\cdot h_l' s'})=e(g, V') \tag{6}$$

是否成立。

若式(5)、式(6)均成立，证明用户身份属性来自环 $C1$ 成员。

第 3 步　验证计算式(2)~式(6)。

$$\frac{e(SK_{\omega_R,2},CT_1)}{e(SK_{\omega_R,0},CT_3)}$$

$$=\frac{e\left(h_2^{\alpha\rho_{\omega_R}}\left(\prod_{j\in\omega_R} g^{\frac{q(j)}{t_j}}\right)^{t}, g^{r'''}\right)}{e\left(g^{t}, \left(\prod_{i\in\omega_R} g^{\frac{q(i)}{t_i}}\right)^{r'''}\right)}$$

$$=\frac{e\left(h_2^{\alpha\rho_{\omega_R}}, g^{r'''}\right)e\left(\left(\prod_{j\in\omega_R} g^{\frac{q(j)}{t_j}}\right)^{t}, g^{r'''}\right)}{e\left(g^{t}, \left(\prod_{i\in\omega_R} g^{\frac{q(i)}{t_i}}\right)^{r'''}\right)}$$

$$=e\left(h_2^{\alpha\rho_{\omega_R}}, g^{r'''}\right)$$

$$=e(h_2,g_1)^{\rho_{\omega_R} r''}$$

$e(CT_5, g)$

$$=e\left(SK_{\omega_s,1}\left(h_1\prod_{i\in\omega_s} g^{\frac{q(i)}{t_i}}\right)^{r'''}, g\right)$$

$$=e\left(g_2^{\alpha\rho_{\omega_s}}\left(\prod_{i\in\omega_s} g^{\frac{q(i)}{t_i}}\right)^{t}, g\right)e\left(\left(h_1\prod_{i\in\omega_R} g^{\frac{q(i)}{t_i}}\right)^{r'''}, g\right)$$

$$=e(g_2^{\alpha\rho_{\omega_s}}, g)e\left(\left(\prod_{i\in\omega_s} g^{\frac{q(i)}{t_i}}\right)^{t}, g\right)e\left(\left(h_1\prod_{i\in\omega_R} g^{\frac{q(i)}{t_i}}\right)^{r'''}, g\right)$$

$$=PK_{\omega_S}\ e(CT_4,\ \prod_{i\in\omega_s} g^{\frac{q(i)}{t_i}})e(CT_1,\ h_1\prod_{j\in\omega_R} g^{\frac{q(j)}{t_j}})$$

$$CT_2\frac{e\left(CT_3,SK_{\omega_R,2}\right)}{e\left(CT_1,SK_{\omega_R,1}\right)}$$

$$=e\left(g_1,h_2\right)^{\rho_{\omega_R}r''}\oplus\left(Ve\left(g_1,g_2\right)^{\rho_{\omega_R}r'''}\right)\cdot\frac{e\left(\left(\prod_{i\in\omega_R}g^{\frac{q(i)}{t_i}}\right)^{r'''},h_2^{\alpha\rho_{\omega_s}}\left(\prod_{j\in\omega_s}g^{\frac{q(j)}{t_j}}\right)^{t}\right)}{e\left(g^{r'''},g_2^{\alpha\rho_{\omega_R}}\left(\prod_{i\in\omega_R}g^{\frac{q(i)}{t_i}}\right)^{t}\right)}$$

$$=e\left(g_1,h_2\right)^{\rho_{\omega_R}r''}\oplus\left(Ve\left(g^{r'''},g_2^{\alpha\rho_{\omega}}\right)\right)\cdot\frac{e\left(\left(\prod_{i\in\omega_R}g^{\frac{q(i)}{t_i}}\right)^{r'''},h_2^{\alpha\rho_{\omega_s}}\left(\prod_{j\in\omega_s}g^{\frac{q(j)}{t_j}}\right)^{t}\right)}{e\left(g^{r'''},g_2^{\alpha\rho_{\omega_R}}\left(\prod_{i\in\omega_R}g^{\frac{q(i)}{t_i}}\right)^{t}\right)}$$

$$=e\left(g_1,h_2\right)^{\rho_{\omega_R}r''}\oplus\left(Ve\left(\prod_{i\in\omega_R}g^{\frac{q(i)}{t_i}}\right)^{r'''},h_2^{\alpha\rho_{\omega_s}}\right)$$

$$=e\left(g_1,h_2\right)^{\rho_{\omega_R}r''}\oplus\left(Ve\left(g_1,h_2\right)^{\rho_{\omega_R}r''}\right)$$

$$=V$$

式(2)~式(4)均成立，式(2)说明盲签密文 CT 有效，式(3)和式(4)说明 CT 和用户属性强不可伪造。

$U_k=E_k^{r_k}/\prod_{l\in c1}U_lE_l=g^{t_kr_ks}/\prod_{l\in c1}U_lg^{t_lh_ls}$，且有

$$\prod_{l'\in\omega_s'\bigcup\omega_R}U_{l'}E_l^{h_l'}$$

$$=(U_{k'}\ E_k^{h'}k')\prod_{l\in\omega_s'\bigcup\omega_R}U_lE_l^{h_l'}$$

$$=E_k^{r_{k'}}E_k^{h_{k'}}$$

$$=g^{t_{k'}(r_{k'}+h_{k'})s'}$$

即可得 $U=g^{s'}$。

$$e(g,\ \prod_{k=1}^{L}U_l\ g^{t_lh_l's'})$$

$$=e(g,g^{t_{k'}(r_{k'}+h_{k'})})$$

$$=e\left(g,g\right)^{t_{k'}(r_{k'}+h_{k'})s'}$$

$$e(g,V')$$

$$=e(g,E_k^{r_{k'}}E_k^{h_{k'}})$$

$$=e(g,g^{t_{k'}(r_{k'}+h_{k'})s'})$$

$$=e\left(g,g\right)^{t_{k'}(r_{k'}+h_{k'})s'}$$

即可得 $e(g,\prod_{k=1}^{L}U_l\ g^{t_l\cdot h_l's'})=e(g,V')$。

式(5)和式(6)均成立，说明用户来自环 $C1$ 成员，源 CSP 不能确信用户的具体身份属性。

4.2 安全分析

在标准模型下，SUIAPRS 方案满足适应性选择密文攻击(IND-SUIAPRS-CCA2)。以用户访问权限为中心，用户自主选择随机数本地生成公钥和完全私钥，PKG 无法推导出用户公钥和完全私钥；去中心化的盲环签密，攻击者即使共谋无法伪造可利用的第二个有效签密消息即强不可伪造；攻击者无法连接签密会话过程、验证签密者真实身份即满足盲性特征。

4.2.1 公钥和完全私钥安全证明

从图 2 中的应用场景和密钥生成的定义，用户从 PKG 获得系统参数和部分私钥，可知：1) 公钥基于盲化因子 ρ_ω 和系统参数生成；2) 完全私钥基于部分私钥、盲化因子 r'和系统参数生成，且只有用户知道盲化因子的来源；3)用户公钥和完全私钥安全取决于盲化因子 r'和 ρ_ω。用户随机向源 CSP 申请认证，每次从 PKG 获得的部分私钥不一样，盲化因子 r'和 ρ_ω 也不一样。因此，PKG 无法从系统参数和部分私钥推导出用户公钥和完全私钥。

4.2.2 SUIAPRS 强不可伪造和盲性证明

如果没有多项式时间概率攻击者 A 在下列游戏中有不可忽略的优势，SUIAPRS 方案具有强不可伪造性和盲性。

系统建立。挑战者 C 运行 setup 算法，并生成 $params^*$和 MSK^*，并向 A 传递 $params^*$。

第一阶段　C 响应 A 的以下任何询问。

extract-partial-private-key-query：当 A 询问属性 ω_s^* 的部分私钥 $D_{\omega_s^*}^*$ 时，C 运行部分密钥生成算法，输入 ω_s^*、$params^*$和 MSK^*，输出 $D_{\omega_s^*}^*$ 响应 A。

centerless-generate-user-key-query：当 A 询问 ω_s^* 的公钥 $PK_{\omega_s^*}^*$，C 首先访问本地数据库是否存在相应入口。如果不存在，C 执行公钥生成算法获得密钥对（$\rho_{\omega_s^*}^*,PK_{\omega_s^*}^*$）且 $PK_{\omega_s^*}^*=e\left(g_1^*,g_2^*\right)^{\rho_{\omega_s^*}^*}$，存储密钥对至本地数据库，返回 $PK_{\omega_s^*}^*$ 响应 A。

extract-private-key-query：当 A 询问 ω_s^* 的完全私钥 $SK_{\omega_s^*}^*$，C 首先访问本地数据库是否存在相应入口。如果不存在，C 首先执行公钥算法，获得密钥对（$\rho_{\omega_s^*}^*$，$PK_{\omega_s^*}^*$）；采用类似 extract-partial-private-

key-query 方法构造一个 $D^*_{\omega_s^*}$。假设 $F(\omega_s^*)\neq 0 \bmod p$，$C$ 选择随机数 $r'^* \in Z_p$，计算

$$SK^*_{\omega_s^*}=(SK^*_{\omega_s^*,1},\ SK^*_{\omega_s^*,2},\ SK^*_{\omega_s^*,0})$$

$$=(D^{\rho^*_{\omega_s^*}}_{\omega_s^*,1}\left(\prod\nolimits_{i\in\omega_s^*} g^{*\frac{q(i)}{t_i}}\right)^{r'^*},$$

$$D^{\rho^*_{\omega_s^*}}_{\omega_s^*,1}\left(\prod\nolimits_{j\in\omega^*} g^{*\frac{q(j)}{t_j}}\right)^{r'^*}, D^{\rho^*_{\omega_s^*}}_{\omega_s^*,1} g^{*r'^*})$$

$$=((g_2^{\alpha^*})^{\rho^*_{\omega_s^*}}\left(\prod\nolimits_{i\in\omega_s^*} g^{*\frac{q(i)}{t_i}}\right)^{t},$$

$$(h_2^{\alpha^*})^{\rho^*_{\omega_s^*}}\left(\prod\nolimits_{j\in\omega_s^*} g^{*\frac{q(j)}{t_j}}\right)^{t}, g^{*t})$$

其中，$t=r^*\rho^*_{\omega_s^*}+r'^*$。

C 存储密钥至本地数据库，返回 $SK^*_{\omega_s^*}$ 响应 A。如果 $F(\omega^*)=0 \bmod p$，C 异常返回并随机选择 β^* 的响应 A。

replace-public-key-query：当 A 具有新的有效公钥 $PK'_{\omega_s^*}{}^*$ 时，要求替代当前公钥 $PK^*_{\omega_s^*}$。C 访问本地数据库查找 $PK^*_{\omega_s^*}$，并用新公钥 $PK'_{\omega_s^*}{}^*$ 取代；如果 $PK^*_{\omega_s^*}$ 不存在，直接赋值 $PK^*_{\omega_s^*}=PK'_{\omega_s^*}{}^*$。

blind-signcryption-query：当 A 询问属性 ω_s^* 的发送者、属性 ω_R^* 的接收者、消息 m^*、环 $C1^*$ 和 $SK^*_{\omega_s^*}$ 的盲签密，C 访问本地数据库查找 $PK^*_{\omega_R^*}$ 和 $SK^*_{\omega_s^*}$，然后执行盲签密算法生成环签密文 CT^* 响应 A。如果必须，C 执行公钥生成算法获得 $PK^*_{\omega_R^*}$、私钥算法获得 $SK^*_{\omega_s^*}$、盲签密算法获得 CT^*，并将 CT^* 发送给 A；如果不能模拟完成，C 异常返回并随机选择 β^* 响应 A。

unsigncryption-query：当 A 询问属性 ω_R^* 的接受者、环签密文 CT^* 和当前公钥 $PK^*_{\omega_R^*}=(g_1^*,g_2^*)^{\rho^*_{\omega_R^*}}$ 的解签密，C 首先执行解签密算法的部分验证。如果验证不成功，C 返回无效终止符 $\perp$；反之，C 访问本地数据库并计算解签密。

C 解密签密文 $CT^*=(C1^*,\ W^*,\ \Omega^*,\ \{U_L^*\}_{k=1}^{L},\ \{E_i^*\}_{i=1}^{d},\{E_j^*\}_{j=1}^{L-d})$，其中，$W^*=(C1^*\ //\ m'''^*\ //\ r'''^*\ //\ U_L^*\ //\ r''''^*)\oplus H(\Omega^*\ //\ X^*\ //\ S^*\ //\ \tilde{S}^*)$ 和 $m'''^*=(CT_1^*,\ CT_2^*,\ CT_3^*,\ CT_4^*, CT_5^*)$，$C$ 获得发送者私钥 $SK^*_{\omega_s^*}=(SK^*_{\omega_S^*,1},\ SK^*_{\omega_s^*,2},\ SK^*_{\omega_s^*,0})$ 和接收者 $\rho^*_{\omega_R^*}$ 及 $PK^*_{\omega_R^*}$。$CT_5^*=SK^*_{\omega_S^*,1}\left(h_1^*\prod_{j\in\omega_S^*} g^{\frac{q(j)}{t_j}}\right)^{r'''^*}$ 和 $CT_1^*=g^{r'''^*}$，在式(2)~式(6)已分别计算出了 $m^*=CT_1^*/e(g_1^{*\rho^*_{\omega_R^*}},\ g_2^{*r'''^*})$，并将 m^* 发送给 A。

挑战阶段。A 提交 2 个属性集 ω_s^* 和 ω_R^*，如果 ω_s^* 在 extract-partial-private-key 没有被询问且 ω_R^* 在 blind-signcryption 没有被询问，那么 A 输出消息 m^* 的伪造密文（$CT^*, C1^*, SK^*_{\omega_R^*}$）并且伪造是有效的。如果 CT^* 是 ω_s^* 签密 m^* 的有效伪造密文，并且发送给 $SK^*_{\omega_R^*}$ 接收者，A 游戏中获胜。在上述游戏中，A 的优势 $\mathrm{Adv}(A)=\Pr[\mathrm{unsigncrypt}(CT^*, C1^*, SK^*_{\omega_R^*})=m^*]$。在以上安全模型中，$A$ 可以生成 m^* 的（$CT^*, C1^*, SK^*_{\omega_R^*}$）有效元组，（$m^*, CT^*$）不是签密询问的输出。因此，假设 CT^* 不是 C 和 A 在询问和伪造阶段的输出，那么 m^* 在签密阶段可能被询问过，方案满足强不可伪造性。

如果对任意的 $\lambda\in N$ 和 A 在多项式时间内在下列游戏中获胜，那么环签密满足盲性。C 生成密钥对（SK_A^*, PK_A^*）并发送给 A。A 提交一个环 $C1^*$ 和 2 个消息 m_0^* 和 m_1^* 及 $H(C1^*,\ m_0^*, m_1^*)$。用户与 A 交互获得 2 个消息的签密，A 选择一个位 $b\leftarrow\{0,\ 1\}$。A 发送签密 CT_b^* 和 CT_{1-b}^*。如果任何交互不能完成或不能验证存在 $H(C1^*,\ m_0^*, m_1^*)=H(C1,\ m_0,\ m_1)$(表示已被询问)，$A$ 的其他签密无效。A 输出 b'，如果 $b=b'$ 将获胜，方案满足盲性。

第二阶段和第一阶段相同类型的询问。

猜测阶段。A 提交一个 b'，如果 $b'=b$，C 输出 $\beta'=1$ 表示 $Z=e(g,g)^{abc}$，否则输出 $\beta'=0$。因此，可以确定如果 $Z\neq e(g,g)^{abc}$，则 Z 是 G_T 中的一个随机值，C 在游戏中获胜。C 的优势为 $\mathrm{Adv}(A)=\left|2\Pr[b'=b]-1\right|$，以可忽略优势赢得了安全游戏。

4.3　性能分析

本节给出 SUIAPRS 方案与文献[24, 25]在通信成本、存储开销和计算效率的比较分析。设 $|p|$ 表示 Z_p 元素规模，$|g|$、$|g_T|$ 表示 G、G_T 元素规模，n_a、n_u 表示系统用户属性数、用户总数，H_a 表示散列函数计算，P_a 表示双线性对计算，$\mathrm{Exp_G}$ 表示 G 上的

指数运算，Exp_{G_T} 表示 G_T 上的指数运算，$|aG|$表示 G 上的 a 元素二进制长度。

4.3.1 通信成本

系统中通信成本主要由密钥和密文产生，如表 2 所示。用户、PKG 和源 CSP 之间的通信成本来自系统参数、主密钥、部分私钥和密文。源 CSP 和用户需要获得部分私钥来生成本地公钥和完全私钥，贡献了和 PKG 之间的通信成本。本文方案，PKG 与源 CSP 和用户的通信成本主要来自系统参数和主私钥，系统参数规模与$|g|$相关，主私钥规模与 n_a 相关；文献[24]通信成本是数字证书发布用户签名私钥，文献[25]通信成本是发布用户私钥，用户私钥规模与$|p|$相关。

本文方案，源 CSP 和用户之间的通信成本主要来自密文。文献[24, 25]通信成本包括密文和消息报头，报头与用户数量成线性关系；密文规模与$|g_T|$相关，报头规模与$|g|$、$|p|$和 n_u、n_a 相关，本文方案密文规模小于文献[24, 25]密文规模。因此，本文方案通信成本低于文献[24, 25]。

表 2 通信成本比较

通信成本	本文方案	文献[24]方案	文献[25]方案
用户和 PKG	$3\|g\|$	$\|g+2n_a g\|$	$2\|g\|+n_a\|g\|$
源 CSP 和 PKG	$3\|g\|+\|g_T\|$	$2\|g\|+\|p\|$	$2\|g\|+2\|p\|$
用户和源 CSP	$\|g_T\|+n_a\|g\|$	$\|g_T\|+\|p\|\|g\|$	$\|g_T\|+n_u\|p\|$

4.3.2 存储开销

系统中每个实体存储开销如表 3 所示，本文方案 PKG 存储开销包含系统参数、通用属性集、主密钥和用户部分私钥，系统参数、主密钥规模与 n_a 呈线性关系；用户和源 CSP 存储开销包含部分私钥、完全私钥、公钥，与$|g|$和$|g_T|$相关。文献[24]中 PKG 存储开销包含用户身份、系统参数、主密钥和用户数字证书，用户数字证书规模与 n_u 呈线性关系；源 CSP 和用户存储开销主要是数字证书、密文、消息头，与 n_u 呈线性关系；文献[25]每个实体还增加了认证密钥，与$|g_T|$相关。

表 3 存储开销比较

实体	本文方案	文献[24]方案	文献[25]方案
PKG	$(2+n_a)\|p\|$	$n_u\|g\|+2\|p\|$	$n_u\|g\|+\log_{n_u}\|p\|$
用户	$(3+n_a)\|g\|$	$(2n_u+1)\|g\|+\log_{n_u}\|p\|$	$n_u\|p\|+3\|g\|$
源 CSP	$3\|g\|+\|g_T\|$	$2\|g_T\|+3\|g\|$	$2\|g_T\|+n_u\|g\|$

4.3.3 计算效率

各系统中计算效率包括计算时间和计算成本，盲环签密与解签密验证服务计算时间主要与用户属性数量呈线性关系，计算成本主要与困难性假设相关。

用户属性数量规模增加、系统计算时间增长率决定了签密和验证的效率。比较计算时间通过仿真实验方法，基于 Intel Dual-Core2 主频 2.6 GHz、Windows 7 和 8 GB 内存，利用版本号为 0.5.14 的密码库(pairing-based cryptography)，利用对称椭圆曲线基域规模为 512 位、植入度为 2 的 α-曲线，并且 α-曲线有 160 位长素数 P，明文规模为 512 kB。系统计算时间与用户拥有属性数量呈线性关系，实验结果如图 3 所示，纵轴表示系统计算时间，横轴表示用户属性数量，本文方案盲环签密与解签密验证服务系统计算时间增长率小于文献[24, 25]方案。

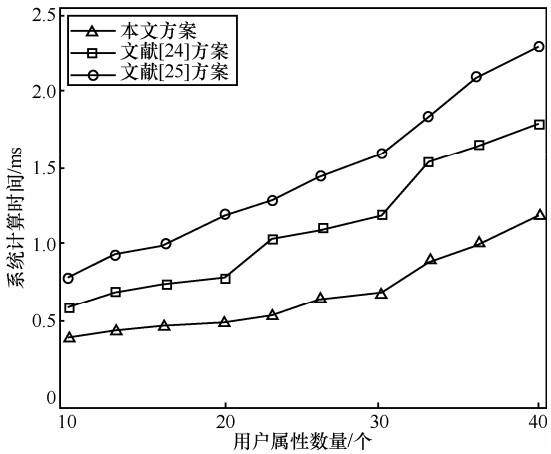

图 3 计算时间比较

在双线性映射和标准模型下，无证书盲环签密方案在计算成本方面有较大改进，如表 4 所示。与文献 [24, 25]方案相比，本文方案在指数运算、散列运算方面优于文献[24, 25]方案。本文方案在 DBDH 困难性假设下，具有适应性选择密文攻击和选择消息攻击下存在属性强不可伪造、密文不可区分，系统计算成本优于文献[24, 25]方案。

表 4 计算成本比较

指标	本文方案	文献[24]方案	文献[25]方案
对运算	$5p_a$	$6p_a$	$5p_a$
指数运算	$3\mathrm{Exp}_G+\mathrm{Exp}_{G_T}$	$2\mathrm{Exp}_G+2\mathrm{Exp}_{G_T}$	$5\mathrm{Exp}_G+\mathrm{Exp}_{G_T}$
散列计算	$2H_a$	$4H_a$	$5H_a$
密文规模	$4\|G\|+\|G_T\|$	$5\|G\|+2\|G_T\|$	$4\|G\|+\|G_T\|$
模型	标准	*RO*	*RO*

综合通信成本、存储开销和计算效率 3 个方面，本文方案系统综合性能优于文献[24, 25]方案。

5　面向云计算的身份认证管理

5.1　盲环签密身份属性保护方案认证管理

以 SPICE 架构为基础，SUIAPRS 方案实际应用场景的身份认证管理架构如图 4 所示。系统包含 5 个组件：注册者、用户、Web 浏览器、源 CSP 和接收 CSP。Web 浏览器代表用户与源 CSP 通过在线交互完成认证。注册者是一个可信第三方，依据用户属性集为每个用户生成部分私钥，不参与认证过程；若没有新用户请求密钥服务，注册者保持脱机状态。用户、接收 CSP 和源 CSP 有部分相同模块，为了区分它们的角色，图 4 中接收 CSP 省去了与源 CSP 相同的一部分组件。同时，源 CSP 也省去了与用户相同的公钥、私钥组件。注册者管理通用属性集，利用 3.2 节算法 1)、2)生成公共参数、主密钥和用户部分私钥，通过安全通道传递给用户，用户保存本地。

当用户通过浏览器向源 CSP 发出服务请求时，源 CSP 返回认证请求，包括身份属性认证；当用户收到认证请求，执行盲环签密 blind- signcryption 算法签密环 $C1$、身份属性子集和消息 M 密文，同时利用$(m,\ \tilde{m}\ ,\ S,\ \tilde{S}\ )$隐藏用户身份属性和$(\ SK_{\omega_s,0}\ ,\ SK_{\omega_s,1}\ )$保护属性、消息完整性；源 CSP 执行解签密 unsigncryption 算法验证用户属于环 $C1$ 成员、属性和密文非伪造、密文有效，利用（$SK_{\omega_R,0}$，$SK_{\omega_R,2}$）验证密文有效，利用 $SK_{\omega_s,1}$ 和（$SK_{\omega_R,1}$，$SK_{\omega_R,2}$）验证属性和密文非伪造，利用属性并集验证用户属于 $C1$ 成员但无法获得真实信息，身份认证通过。用户通过源 CSP 身份认证，同时也必须通过接收 CSP 的认证。源 CSP 和接收 CSP 组成另一个环 $C2$，通过类似的方法通过接收 CSP 的验证，用户可以获得多个源 CSP 和接收 CSP 联合提供的存储和应用服务，图 4 提供了一个认证管理基本框架。

5.2　安全隐私和功能需求

1) 以用户访问权限为中心。基于环签密的身份属性保护方案，用户根据属性向注册者申请部分私钥，用户随机选择秘密值，依据系统公共参数生成公钥，依据系统主密钥、部分私钥生成完全私钥，注册者无法获得用户完全私钥；用户可以自主动态更新秘密值，随机申请源 CSP 服务。

2) 强不可伪造性。强不可伪造性是基于 DBDH 困难性假设、适应性选择密文攻击和选择消息攻击，散列运算、双线性对运算、点乘运算和指数运

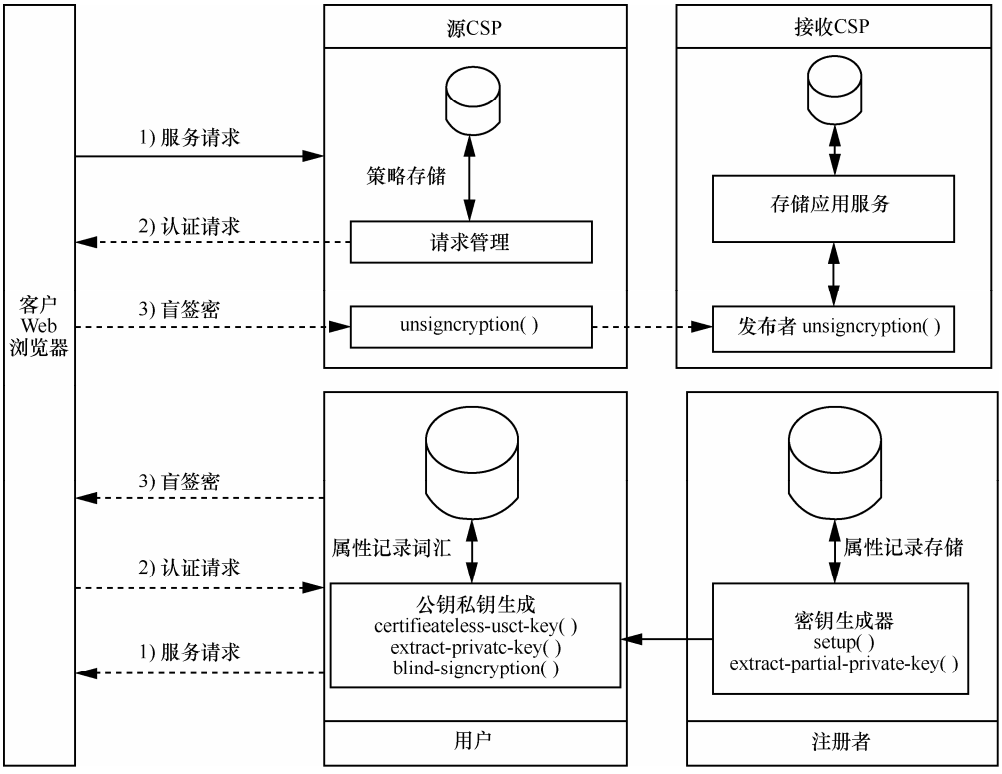

图 4　认证管理架构

算的高效性，使不存在多项式概率时间敌手 A 以一个不可忽略优势伪造密文以获得用户身份属性和完全私钥。

3) 盲性。用户对身份属性采取基于环的盲签密，源 CSP 作为环成员只能验证用户来自环内成员，身份是真实的，无法获得用户的具体身份属性信息。同理，注册者作为可信第三方控制属性集，环签密方法使注册者无法获得用户完全私钥。

6 结束语

身份属性安全是云计算安全的焦点，DIM 作为身份属性的管理者是重要的安全基础设施之一。基于环签密的身份属性保护系统，以随机语言模型下的属性环签密为基础，对标准模型下的无证书签密方案进行了相关扩展，融合了标准模型下的身份签密和盲环签名，解决了密钥管理中心瓶颈、身份属性泄露和密文伪造问题。系统所有操作均在脱机状态下完成，用户在申请密钥服务之前降低了和注册者的交互通信；通过环签密与验证的方法结合源 CSP 认证身份属性，简化了身份认证的计算和通信复杂度。提出了基于此方案的云环境用户认证管理架构。SUIAPRS 方案简化了群签名的指数运算次数，消除了证书存储负载，降低了环签密算法和解签密算法的运算负载，但增加了标量点乘运算次数和用户密钥本地存储开销，因此如何降低综合负载将作为进一步的研究方向。

参考文献：

[1] MICHAEL A, ARMANDO F, REAN G. Above the Clouds: a Berkeley View of Cloud Computing[R]. Berkeley:University of California, UC Berkeley Reliable Adaptive Distributed Systems Laboratory, 2009.

[2] 童晓渝, 张云勇, 徐雷. 智能普适网络[J]. 通信学报, 2011, 32(7): 182-188.
TONG X Y, ZHANG Y Y, XU L. Intelligent ubiquitous network[J]. Journal on Communications, 2011, 32(7): 182-188.

[3] ANGEL J M, INY K. Spontaneous task composition in urban computing environments based on social, spatial and temporal aspects[J]. Engineering Applications of Artificial Intelligence, 2011, 24: 1446- 1460.

[4] ZHANG H G, LI C L, TANG M. Evolutionary cryptography against multidimensional linear cryptanalysis[J]. Sci China InfSci, 2011, 54(12): 2565-2577.

[5] WANG H Z, ZHANG H G, *et al*. Extended multivariate public key crypto systems with secure encryption function[J]. Sci China InfSci, 2011, 54(6): 1161-1171.

[6] ZHANG H G, LI C L, TANG M. Capability of evolutionary cryptosystems against differential cryptanalysis[J]. Sci China InfSci, 2011, 54(10): 1991-2000.

[7] TANG M, ZHANG H G, *et al*. Evolutionary chipers against differential power analysis and differential fault analysis[J].Sci China InfSci, 2012, 55(4): 911-920.

[8] 彭长根, 田有亮, 张豹等. 基于同态加密体制的通用可传递签名方案[J]. 通信学报, 2013, 34(11): 18-25.
PENG C G, TIAN Y L, ZHANG B, *et al*. General transitive signature scheme based on homomorphism encryption[J]. Journal on Communications, 2013, 34(11):18-25.

[9] FENG D G, ZHANG M, *et al*. Study on cloud computing security[J]. Journal of Software, 2011, 22(1):71-83.

[10] MARK D R. Cloud computing security: the scientific challenge, and a survey of solutions[J]. The Journal of Systems and Software, 2013, 86: 2263-2268.

[11] HASSAN T, JAMES B D, *et al*. Security and privacy challenges incloud computing environments[J]. IEEE Security and Privacy, 2010, 10:24-31.

[12] SHAREEFULI, HARALAMBOS M, *et al*. Model based process to support security and privacy requirements engineering[J]. International Journal of Secure Software Engineering, 2012, 3:1-3.

[13] NIR K. Privacy and security issues in cloud computing: the role of institutions and institutional evolution[J]. Telecommunications Policy, 2013, 37: 372-386.

[14] ALLIANCE C S. The notorious nine cloud computing top threats in 2013[EB/OL]. http://cloudsecurityalliance.org/research/top-threats.

[15] BERTINO E, PACI F, *et al*. Privacy preserving digital identity management for cloud computing[J]. IEEE Data Eng Bull, 2009, 32(1): 21-27.

[16] PELIN A, BHARAT B, *et al*. An entity-centric approach for privacy and identity management in cloud computing[A]. Proc of 29th IEEE Symposium on Reliable Distributed Systems[C]. 2010.177-183.

[17] HUSSAIN M. The Design and Applications of a Privacy-Preserving Identity and Trust-Management System[D]. Canada:School of Computing, Queen's University, 2010.

[18] CELESTI A, TUSA F, *et al*. Security and cloud computing: intercloud identity management infrastructure[A]. Proc of 2010 Workshops on Enabling Technologies[C]. 2010.263-265.

[19] ROHIT R, BHARAT B, *et al*. Protection of identity information in cloud computing without trusted third party[A]. Proc of the 29th IEEE Symposium on Reliable Distributed Systems[C]. 2010. 368-372.

[20] GOVINDA K, SATHIYAMOORTHY D E. Identity anonymization and secure data storage using group signature in private cloud[J]. Procedia Technology, 2012, 4: 495-499.

[21] HARALAMBOS M, SHAREEFUL I, *et al*. A framework to support selection of cloud providers based on security and privacy requirements[J]. The Journal of Systems and Software, 2013, 86:2276-2293.

[22] WANG H. Privacy preserving data sharing in cloud computing[J]. Journal of Computer Science and Technology, 2010, 25(3):401-414.

[23] CHUANG I-HSUN, LI S H, *et al*. An effective privacy protection scheme for cloud computing[A]. Proc of 13th International Conference on Advanced Communication Technology[C]. PyeongChang, 2011. 260-265.

[24] SHERMAN S M C, HE Y J, *et al*. Simple privacy-preserving identity-management for cloud environment[A]. Proc of ACNS 2012[C]. Berlin Heidelberg, 2012.526-543.

[25] WEI L F, ZHU H J, *et al*. Security and privacy for storage and computation in cloud computing[J]. Information Sciences, 2014, 258:371-386.

[26] ADEELA W, ASAD R, *et al*. A framework for preservation of cloud users' data privacy using dynamic reconstruction of metadata[J]. Journal of Network and Computer Applications, 2013, 36: 235-248.

[27] GUO Z Z, LI M C, FAN X X. Attribute-based ring signcryption scheme[J]. Security and Comm Networks, 2013, 6:790-796.

[28] LIU Z H, HU Y P, *et al*. Certificatelesssigncryption scheme in the standard model[J]. Information Sciences, 2010, 180:452-464.

[29] ESSAM G. Sub-linear Blind Ring Signatures without Random Oracles[R]. Cryptology ePrint Archive, Report 2013/612, 2013.

[30] SHARMILA S D S, SREE V, *et al*. ID Based Signcryption Scheme in Standard Model[R]. Cryptology ePrint Archive, Report 2012/392, 2013.

[31] DAN B, MATT F. Identity-based encryption from the weil pairing[A]. Proc of CRYPTO 2001[C]. Berlin Heidelberg, 2001.213-229.

作者简介：

李拴保（1972-），男，河南安阳人，武汉大学博士生，主要研究方向为大数据、云计算、信息安全。

傅建明[通信作者]（1969-），男，湖南长沙人，武汉大学教授、博士生导师，主要研究方向为可信计算、软件安全、网络安全。E-mail:jmfu@shu.edu.cn。

张焕国（1945-），男，河北元氏人，武汉大学教授、博士生导师，主要研究方向为密码学、可信计算、信息安全。

陈晶（1981-），男，湖北武汉人，武汉大学副教授、博士生导师，主要研究方向为网络安全、分布式系统安全。

王晶（1988-），女，广西桂林人，武汉大学博士生，主要研究方向为属性密码学、云计算安全、物联网安全。

任必军（1959-），男，河南沁阳人，河南财政税务高等专科学校副教授，主要研究方向为密码学、计算机算法。