云环境下基于属性的用户权限管理研究

李拴保[1,2,3] 范乃英[3] 傅建明[1,2] 祁慧敏[3] 刘 芊[3]
(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)[1]
(武汉大学计算机学院 武汉 430072)[2] (河南财政税务高等专科学校 郑州 451464)[3]

摘 要 用户权限分配是云计算服务的重要难题之一,提出了一种基于属性的用户权限管理方案。该方案以云服务中的新用户密钥分配为研究对象,论述了多方协同的用户签名验证解密管理机制,数据所有者和授权者共同选择属性集,数据所有者基于属性集定义密文访问结构,从而用户只有通过授权者认证才能获得解密密钥,达到用户权限升级与降级同步管理的目的。另外,本方案以群属性集更新为中心设计CP-ABE群签名验证机制,令数据所有者、用户和授权者组成群;基于群和自身属性用户可对消息签名以及公开验证,用以保护密文数据的细粒度访问控制。最后,给出签名有效性和不可伪造的证明结果。

关键词 密文策略属性加密,签名,验证,不可伪造
中图法分类号 TP393.08 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.09.028

Study on User Permissions Management Based on Attribute for Cloud Environment

LI Shuan-bao[1,2,3] FAN Nai-ying[3] FU Jian-ming[1,2] QI Hui-min[3] LIU Qian[3]
(Key Lab of Aerospace Information Security and Trusted Computing Ministry of Education, Wuhan University, Wuhan 430072, China)[1]
(School of Computer, Wuhan University, Wuhan 430072, China)[2] (Henan College of Finance and Taxation, Zhengzhou 451464, China)[3]

Abstract User permissions assignment is one of the important challenges of cloud computing services. We proposed an user permissions management scheme based on an attribute. The program make the key distribution of new users in cloud services as the study object, which discusses the multi-collaborative signature verification and decryption management mechanism. Data owners and authority commonly decide on attribute set, and data owner defines ciphertext access structure based on the attribute set, so that only authorized users who hasbeen certified can get the decryption key, to upgrade and downgrade synchronously user permissions management. In addition, we designed CP-ABE group signature verification decryption mechanism by updating-centric for group attribute set, which constitutes group of data owners, users and authority. Users can sign message and publicly verifiability by combining group and own attribute so that the fine- grained access control of ciphertext data can be protected. At last, the validity and unforgeability of the signature can be proved.

Keywords CP-ABE, Signature, Verify, Unforgeability

1 引言

云计算[1,19]作为一种新型计算模式,通过对网络可访问的计算资源共享池灵活整合和动态配置,为用户提供面向需求的数据共享服务,在智慧城市[2]等领域有着广泛的应用。许多用户把私有数据迁移云中,可在任何时间、任何地点访问;但是,用户面临私有数据泄露的威胁,希望实施灵活的访问控制策略。文献[4-7,9]提出了共享数据加密访问控制系统[8],基于用户角色或属性提供差别访问服务;但是,其不适用于云计算服务环境,因为云服务提供者、用户和数据所有者属于不同的可信域,数据所有者希望掌控用户访问策略的制定。

科学家提出了云环境下的访问控制模型,基于环境不同属性定义访问控制策略,数据保护基于密码方法实现;基于属性加密(Attribute-Based Encryption, ABE)概念满足上述需求。ABE的基本特点是访问控制基于加密数据的访问策略、属性关联私钥或密文。KP-ABE属性加密方案的访问结构关联用户私钥、密文关联属性集;当且仅当属性集满足访问结构,用户才可以解密密文,但是加密者不能直接控制谁能访问密文数据。CP-ABE与KP-ABE角色相反,用户私钥关联属性集、密文关联访问结构,数据加密者直接决定谁能访问密文数据。例如,用户私钥关联属性集$\{a,b,c,d,e,f\}$,访问结构定义$a\vee(b\wedge c)$;数据基于$a\vee(b\wedge c)$加密,只有拥有属性a、b、c的用户才能解密密文。不同用户依据每个安全策略允许解

到稿日期:2014-01-10 返修日期:2014-02-26 本文受国家自然科学基金(61373168,61202387),教育部高等学校博士学科点专项科研基金(20120141110002),河南省软科学研究计划(132400410905,132400410979,142400410270)资助。
李拴保(1972—),男,博士生,CCF会员,主要研究方向为大数据、云计算、信息安全,E-mail:phdfuli@126.com;范乃英 女,副教授,主要研究方向为软件工程;傅建明 教授,博士生导师,主要研究方向为网络安全、可信计算、软件安全。

密不同的数据片，可以阻止非授权的数据访问。这些特点，使得 CP-ABE 非常适合云环境下大规模密文数据的访问控制服务。

云环境中，直接应用 CP-ABE 可以控制密文的用户访问权限，但是面临属性和用户撤销困难。因为 ABE 系统的每个属性由多个用户共享，任何属性或单个用户的撤销都会影响共享属性的其它用户；特别是，用户权限升级或降级，共享属性更新直接导致用户密钥失效或系统安全降级。因此，本文主要解决云环境下利用 CP-ABE 管理用户权限这一难题。

1.1 相关工作

ABE 概念由文献[10]提出，形成了两种实现方式：CP-ABE[12]和 KP-ABE[11]。CP-ABE 比 KP-ABE 更适合云计算体系架构，因为数据所有者直接决定属性访问结构以及通过公共属性加密数据。CP-ABE 系统用户私钥嵌入失效时间属性[13]，降低用户的密文访问权限，这种周期性访问控制方法要求所有用户更新私钥而导致系统效率低下。CP-ABE 和 PRE 组合[14-17]，授权者定义用户属性集和属性访问结构，控制部分属性撤销；这种方案可以立即降低用户访问权限，但无法获得规模化和细粒度访问控制。广播、CP-ABE 和属性分割组合[18,20]，数据所有者直接定义授权用户集合和属性访问结构，从系统级撤销用户访问权限；但数据所有者无法控制云服务器中密文的更新。文献[23]提出了 CP-ABE 系统分割用户属性集，从属性级来撤销包含属性子集的用户访问权限，但会影响具有相同属性子集的用户访问。文献[28-30]引入了 ABE 和群签名组合的基于属性用户权限降级方案，但是仅仅针对已有访问权限的原有用户，而对于新用户的访问权限没有详细定义。文献[21,22]提出了 CP-ABE 和属性群密钥组合，授权者从属性级撤销用户访问权限；但是云服务器需要更新属性的群密钥，增加了计算成本。云计算环境下，服务器不是完全可信；CP-ABE 属性撤销和用户撤销方法只能降低用户的访问权限，无法升级用户的访问权限。因此，CP-ABE 和群签名组合的用户权限管理仍是一个开放性难题。

1.2 本文贡献

本文考虑的云服务应用场景如图 1 所示，不可信云服务器永远在线，授权者(Authority)为用户提供密钥服务，数据所有者(Owner)外包加密数据于云服务器，用户(User)获得授权者验证后解密密文。以图 1 应用场景为基本架构，用户权限管理方案来源于扩展 CP-ABE 属性加密[12]和群加入[24]方案，并且融合群签名[27]和群签名撤销[25]机制。授权者、用户和数据所有者组成群，授权者允许用户代表群对数据签名，授权者验证签名来鉴别用户的真实身份并分发解密密钥；用户依据私钥属性满足密文访问结构解密密文。文献[23,30]通过 CP-ABE 和用户群密钥分发实现原有用户访问权限降级，取得了细粒度访问控制。本文将授权者、用户和数据所有者组成群，授权者作为群管理员负责通用属性集管理和新用户权限升降级管理，数据所有者定义属性访问结构和密文更新。首先，引入 CP-ABE 和群属性集更新方法，用户自主加群，授权者更新群属性集，并为新用户分发群私钥，升级其访问权限；其次，引入群签名方法，用户基于群签名消息，授权者验证签名，群签名方法抵制用户共谋获得访问权限；最后，引入群撤销方法，授权者对未通过验证的用户撤销群私钥，抵制群成员身份伪装。

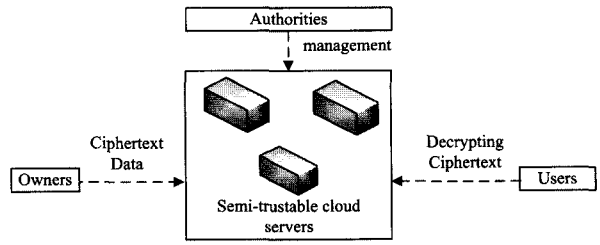

图 1 云服务应用场景

2 预备知识

2.1 双线性映射

本文设计的安全方案基于双线性映射及双线性映射群[26]，其基本原理：假设$\mathbb{G}$和$\mathbb{G}_T$是素数 p 阶的加法、乘法循环群，g 是$\mathbb{G}$的生成元，$e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$是一个双线性映射。双线性映射 e 的基本属性：对任意的 $u,v\in\mathbb{G}$ 和 $a,b\in\mathbb{Z}$，总有 $e(u^a,v^b)=e(u,v)^{ab}$；$e(g,g)\neq 1$；任取 $p,q\in\mathbb{G}_T$，存在有效算法可计算 $e(p,q)$。

2.2 计算性假设

判定双线性 Diffie-Hellman 问题，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[26]定义如下：选择$\mathbb{G}$的随机生成器 g 和随机指数 $a,b,s\in\mathbb{Z}_p$。若将一个元组$(g,g^a,g^b,g^s)\in\mathbb{G}^4$和一个元素 $z\in\mathbb{G}_T$作为输入，则将决定 $z=e(g,g)^{abs}$的输出。如果 $|P_r[\beta(g,g^a,g^b,g^s,e(g,g)^{abs})=0]-P_r[\beta(g,g^a,g^b,g^s,z)=0]|\geqslant\varepsilon$，存在一个算法 β 输出 $b\in\{0,1\}$，在$\mathbb{G}$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$\mathbb{G}$上成立。

3 用户权限管理系统与安全模型

3.1 系统模型

本文以图 1 应用场景为框架的云环境用户权限管理系统包括 4 个实体：用户、云服务器(Cloud Server)、数据所有者和授权者。通过扩展 CP-ABE[12]和群属性集更新[24]方案，并且融合群签名[27]和群属性撤销[25]机制，构造基于属性的 CP-ABE 群签名方案，管理用户权限的升级与降级。用户权限管理 CP-ABE 群签名方案，群$\mathbb{Q}$由 Owner、User 和 Authority 的属性组成，即$\mathbb{Q}=\omega_1\cup\omega_2\cup\cdots\cup\omega_n$。Authority 管理通用属性集 U、系统公共参数 spara 和主密钥 msk，User 自定义属性集 ω 向 Authority 申请密文访问权限。

Authority 根据 User 在系统中的角色对其属性赋权、撤销和重新赋权；当用户获得属性权限时，授权者分发解密密钥和管理属性版本；当属性被撤销时，Authority 更新撤销属性版本号，产生相应更新密钥；更新密钥用于非撤销用户的私钥更新和服务器的密文更新。

Owner 定义基于属性 ψ 的访问结构$\mathbb{A}$，数据基于$\mathbb{A}$加密并迁移至云服务器。云服务器存储数据，不实施数据访问控

制。密文被系统中合法用户访问，访问控制基于签名验证方法，用户属性集满足A才能解密密文。

依据在系统中的角色，每个User被赋予一组属性。由于User角色变化，User属性集可以动态改变。当User权限降级时，部分属性被撤销；当升级时，属性被扩展或重新赋予。只有User属性满足密文关联访问策略A时，才可以解密密文。

3.2 基于属性的用户权限管理框架

基于属性的用户权限管理(User Authority Management Based on Attribute，UAMBA)框架定义，包含以下8个算法。第一、二、四、六和七个算法由Authority运行，第三个算法由Owner运行，第五、八个算法由User运行。

定义1 基于属性的用户权限管理方案是下列算法的集合：Setup，User-Join，Authority-Keygen，Owner-Sign，User-Verify-Decrypt，Authority-Open和Authority-Revoke，其中Join用于新用户入群而Revoke用于用户退出群。

(1)初始化算法 Setup(k)：算法由Authority运行，给定一个安全参数k，Authority选择随机数α作为输入；算法输出主密钥msk和公共参数$spara$，Authority保存msk作为秘密值。User、Owner和Authority基于属性组成群$\mathbb{Q}=\omega_1\cup\cdots\cup\omega_n$，Authority为群$\mathbb{Q}$管理员。

(2)用户加入群算法 Authority-User-Join($spara$，msk，$\mathbb{Q}$，ω')：算法由Authority运行，输入公共参数$spara$、主私钥msk、群$\mathbb{Q}$、User的属性集ω'，输出新群$\mathbb{Q}'=\mathbb{Q}\cup\omega'$，User成为群$\mathbb{Q}'$的新成员，并将$\mathbb{Q}'$发送给群内所有成员。

(3)数据加密算法 Owner-Encrypt($\mathbb{Q}'$，$spara$，$\mathbb{A}$，M)：算法由Owner运行，输入公共参数$spara$、群$\mathbb{Q}'$、消息M和基于属性集$\psi\subset\mathbb{Q}$的访问结构$\mathbb{A}$，输出密文CT；通过秘密通道将ψ传送给Authority。

(4)密钥生成算法 Authority-Keygen($spara$，msk，n，$\mathbb{Q}'$，ω')：算法由Authority运行，输入公共参数$spara$、用户数n、群$\mathbb{Q}'$和ω'，输出基于属性集$\mathbb{Q}'$的公钥gpk和拥有属性ω'的私钥$gsk_{\omega'}$。

(5)签名算法 User-Sign($\mathbb{Q}'$，gpk，M，$gsk_{\omega'}$)：算法由User运行，输入群$\mathbb{Q}'$、群公钥gpk、消息M和用户私钥$gsk_{\omega'}$，输出群签名σ。

(6)验证算法 Authority-Verify(σ，gpk，M)：算法由Authority运行，系统输入签名σ、群公钥gpk、消息M，输出用户验证签名。如果σ有效，输出“valid”，否则输出“Invalid”。

(7)撤销算法 Authority-Revoke-User($spara$，msk，i，φ)：算法由Authority运行，系统输入用户身份指数i和属性集φ，输出用户i被撤销。

(8)解密算法 User-Decrypt(CT，$spara$，msk，i，$gsk_{\omega'}$)：算法由User运行，系统输入密文CT、公共参数$spara$、主私钥msk、用户身份指数i和用户私钥$gsk_{\omega'}$，属性集ω'满足密文访问结构$\mathbb{A}$，输出明文M。

3.3 安全模型

UAMBA安全假设：①对于没有访问权限的用户，允许加群签名认证访问云服务器；②对于已有访问权限的用户，允许撤销用户部分属性，降低访问权限；③用户是不可信的，共谋伪造签名获得访问权限。系统安全游戏规则描述如下。

初始化(Init) 攻击者$\mathcal{A}$选择一个属性树Γ发送给挑战者$\mathcal{C}$。

系统建立(Setup) 挑战者$\mathcal{C}$运行算法Setup和Authority-Keygen，生成基于属性树Γ的公钥gpk和n个私钥基$gsk_{[n]}$。

第一阶段(Phase 1) $\mathcal{A}$执行多项式数量级的适应性私钥、签名和撤销询问，$\mathcal{C}$运行私钥、签名和撤销算法来响应$\mathcal{A}$。

(1)在运行私钥算法过程中，$\mathcal{A}$发送一个指数i和属性集γ_i，$\mathcal{C}$以一个私钥gsk_{γ_i}响应。

(2)在运行签名算法过程中，$\mathcal{A}$发送一个消息M、用户指数i和满足Γ的属性集ω_i，$\mathcal{C}$以签名σ响应。

(3)在运行撤销算法过程中，$\mathcal{C}$提交一个指数i和属性集ϕ，获得一个更新的撤销属性集合R。

挑战阶段(Challenge) $\mathcal{A}$发送两个元组(i_0,M,ω)、(i_1,M,ω)，$\mathcal{C}$随机选择一个$b\in(0,1)$，生成一个签名σ_b来响应$\mathcal{A}$。

第二阶段(Phase 2)和第一阶段一样。

猜测阶段(Guess) 最后，$\mathcal{A}$提交一个$b'\in(0,1)$。如果$b'=b$，那么$\mathcal{A}$在游戏中获胜；否则，失败。攻击者$\mathcal{A}$的优势定义为$\mathrm{adv}(\mathcal{A})=p_r[b'=b]-\frac{1}{2}$，其中$p_r[b'=b]$表示$b'=b$的概率。

定义2 一个基于属性的用户权限管理方案在适应性选择消息攻击(adaptive chosen-message Attack)下是安全的，如果任何多项式时间算法攻击者在IND-UAMBA-CCA2游戏中获胜的概率最多具备一个可忽略的优势。

4 UAMBA方案具体构造、性能比较与安全证明

4.1 具体构造

在标准模型下，用户权限管理方案涉及3方：User、Owner和Authority，它们来自于扩展CP-ABE与群签名加入[12,24]方案以及融合群签名与撤销[25,27]机制。Authority管理通用属性集、生成公共参数与主密钥；User自定义属性集ω并向Authority申请密文访问权限，Authority根据User角色为属性赋权并分发签名私钥；Authority作为群$\mathbb{Q}$管理员，验证User属性并为其提供服务。具体构造及应用包括6个阶段：用户权限管理系统建立阶段、User提升权限服务阶段、Owner数据加密服务阶段、Authority密钥服务阶段、User签名服务阶段、验证撤销与解密服务阶段，如下所述。

4.1.1 用户权限管理系统建立阶段

云环境下基于属性的用户权限管理系统中，Authority负责群$\mathbb{Q}$系统参数、密钥生成环境的初始化，为User访问云服务提供密钥准备。

第一步 定义拉格朗日插值公式$\Delta_{i,s}$，用于乘法循环群签名与验证；对任意$i\in\mathbb{Z}_p$，假设S是$\mathbb{Z}_p$中的元素集合。

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

第二步 定义乘法循环群，基于User、Owner和Authority的属性构造一个群$\mathbb{Q}=\omega_1\cup\cdots\cup\omega_n$。

第三步　Setup(k)算法初始化，给定安全参数 k，Authority选择素数 p 的双线性乘法循环群$\mathbb{G}_0$、$\mathbb{G}_T$，双线性映射 $e:\mathbb{G}_0\times\mathbb{G}_0\to\mathbb{G}_T$，$g$ 是$\mathbb{G}_0$的一个生成元。

第四步　计算系统参数和主密钥，Authority 随机选择 $h\in\mathbb{G}_0$，ζ_1、ζ_2、α、$\beta\in\mathbb{Z}_p$；选择 u、v、ω、$\eta\in\mathbb{G}_0$，定义 $U^{\zeta_1}=V^{\zeta_2}=h$，$\omega=g^{\beta}$，$\eta=g^{\alpha}$；假设通用属性集合$\mathbb{U}=\{1,\cdots,n\}$满足拉格朗日插值式(1)，对每一个属性 $j\in\mathbb{U}$ 有 $t_j\in\mathbb{Z}_p$且存在 $t_j=\beta/1-\alpha$。

第五步　定义密码学哈希函数 $H:\{0,1\}^*\to\mathbb{Z}_p$，用于抵制用户之间共谋。

第六步　Authority 发布公共系统参数 $spara=\{\mathbb{G}_0,\mathbb{G}_T,e,g,H,h,u,v,\omega,\alpha,\beta,e(g,g)^{\alpha}\}$，保存主密钥 $msk=\{\eta,\{t_j\}_{j=1}^{n}\}$。

4.1.2　User 提升权限服务阶段

Authority 为新入群 User 分配签名密钥，用户用于解密云服务器中的密文。

第一步　用户自定义属性集 ω_z，通过安全通道向 Authority 发送 ω_z，申请加入群$\mathbb{Q}$。

第二步　Authority-User-Join($spara$,msk,$\mathbb{Q}$,ω_z)算法初始化，Authority 验证 $\omega_z\cap\omega_i$ 非空且$\omega_z\neq\omega_i$(ω_i 表示群内已有成员)；随机选择 γ、$t_z\in\mathbb{Z}_p$($1\leqslant z\leqslant n$)，计算 $\sigma=g^{1/\gamma+t_z}$，元组(γ,t_z,σ)发送给用户。

第三步　用户验证 $e(\sigma,\eta g^{\eta\beta}\omega^{t_z})=e(\omega,\eta)$成立，用户加群成功；同时，向 Authority 发送 $H(\omega_z,\gamma,t_z,\sigma)$。

第四步　Authority 输出一个新群$\hat{\mathbb{Q}}=\mathbb{Q}\cup\omega_z$，具有属性集 ω_z 的用户成为群$\hat{\mathbb{Q}}$的成员。

4.1.3　Owner 数据加密服务阶段

Owner 和 Authority 共同选择属性集 $\psi\subset\mathbb{Q}$，Owner 定义基于 ψ 的密文访问结构$\mathbb{A}$，加密基于新群$\hat{\mathbb{Q}}$、$\mathbb{A}$和公共参数消息 m，输出密文 CT 迁移云服务器中。

第一步　Owner-Encrypt($\hat{\mathbb{Q}}$,$spara$,$\mathbb{A}$,m)算法初始化，算法基于属性树$\mathbb{A}$为每一个节点 x 选择一个多项式 q_x，q_x 起始于树根节点 R，自上而下；对每一个节点 x，门限值为 k_x，q_x 度为 k_x，并且有 $d_x=k_x-1$。

第二步　算法随机选择 $s\in\mathbb{Z}_p$，使得 $q_R(0)=s$；随机选择另一点 x，使得有 $q_x(0)=q_{parent(x)}(index(x))$，选择 d_x 其它点完整地定义 q_x。

第三步　设$\mathbb{Y}$为属性树$\mathbb{A}$的叶子节点集合，计算基于树访问结构$\mathbb{A}$的密文，$c_0=m\,e(g,g)^{\alpha s}$，$c_1=\omega^{s}$，$c_2=g^{q_y(0)}(\forall y\in\mathbb{Y})$，$c_3=H(att(y))^{q_y(0)}(\forall y\in\mathbb{Y})$；计算 $c''=H(\hat{\mathbb{Q}},c_0,c_1,c_2,c_3)$，系统输出密文 $CT=\{\hat{\mathbb{Q}},\mathbb{A},c_0,c_1,c_2,c_3,c''\}$。

4.1.4　Authority 密钥服务阶段

Authority 为密文访问结构$\mathbb{A}$生成一个群公钥 gpk，为每个用户生成一个群私钥 $gsk[j]$(j 表示属性为 ω_j 的用户)。

第一步　Authority-Keygen($spara$,msk,n,$\mathbb{A}$,msk,$\hat{\mathbb{Q}}$,ω_j)算法初始化，系统选择随机数 r、$r_j\in\mathbb{Z}_p$，对每一个属性 $j\in\omega_j$，计算 $D_j=g^{\gamma}H(j)^{r_j}$，$\hat{D}_j=g^{r_j}$。

第二步　系统利用 β 为每个用户 ω_j($1\leqslant j\leqslant n$)产生私钥基 $gsk[j]_{base}=\langle A_j,X_j\rangle$，随机数 $X_j\in\mathbb{Z}_p$，$A_j=g^{1/\beta+x_j}$。

第三步　系统选择多项式 q_{node}，度 $d_{node}=k_{node}-1$ 为属性树$\mathbb{A}$的每个节点，k_{node}为节点门限。设 $q_{root}(0)=\beta$，$q_{node}(0)=q_{parent}(\mathrm{index}(node))$，$\hat{\mathbb{Q}}$ 访问结构$\mathbb{A}$的公钥 $gpk=\{g,\hat{\mathbb{Q}},D_{leaf_1},\cdots,D_{leaf_k},h_1,\cdots,h_k\}$，其中 $D_{leaf_j}=g^{q_{leaf_j}/t_{leaf_j}}$，$h_j=h^{t_j}$。

第四步　计算用户 ω_j 每一个属性 $i\in\beta$ 的私钥，计算 $T_{j,i}=A_j^{t_i}$，用户 ω_j 的私钥为 $gsk[j]=\langle\omega_j,D,D_j,\hat{D}_j,A_j,x_j,T_{j,1},\cdots,T_{j,n}\rangle$，其中 n 为 β 的规模，$D=g^{\alpha+\gamma/\beta}$。

4.1.5　User 签名服务阶段

用户签名消息向 Authority 申请密文访问权限。

第一步　User-Sign($\hat{\mathbb{Q}}$,gpk,m,$gsk_{\omega'}$)算法初始化，系统选择群$\hat{\mathbb{Q}}$、公钥 gpk、私钥 $gsk[j]$和消息 m，选择随机数 $\rho\in\mathbb{Z}_p$，计算$\hat{u}=H(u,gpk,m,\hat{\mathbb{Q}},\rho)$，$\hat{v}=H(v,gpk,m,\hat{\mathbb{Q}},\rho)$。

第二步　系统计算 $\sigma_1=\hat{u}^{\alpha}$，$\sigma_2=A_j\cdot\hat{v}^{\beta}$，$\sigma_3=T_{j,i}\cdot\hat{v}^{\beta}\cdot e(A_j^{t_i},D_j)\cdot e(\hat{v}^{\beta},\hat{D}_j)$。

第三步　设 $y=X_j\cdot\alpha$，系统随机选择 λ_α、λ_x、$\lambda_y\in\mathbb{Z}_p$，计算 $y_1=\hat{u}^{\lambda_\alpha}$，$y_2=e(\sigma_2,g)^{\lambda_x}\cdot e(\hat{u},\hat{v})^{-\lambda_\alpha}\cdot e(\hat{v},g)^{-\lambda_y}$，$y_3=\sigma_1^{\lambda_x}\cdot\hat{u}^{-\lambda_y}$。

第四步　计算 $C=H(gpk,m,\rho,\sigma_1,\sigma_2,y_1,y_2,y_3)$，设 $T_\alpha=\lambda_\alpha+C\alpha$，$T_x=\lambda_x+CX_j$，$T_y=\lambda_y+Cy$。系统输出签名 $\sigma=(\hat{\mathbb{Q}},\sigma_1,\sigma_2,\sigma_3,C,T_\alpha,T_x,T_y)$。

4.1.6　验证撤销与解密服务阶段

Authority 验证用户的签名，分派用户解密私钥；否则，从群$\hat{\mathbb{Q}}$中撤销用户身份与属性。用户签名通过 Authority 验证，可以解密密文。

第一步　为验证用户签名，系统定义一个递归算法 $Ver_{node}(leaf)=\dfrac{e(\sigma_3,D_j\hat{D}_j)}{\sigma_2}=e(A_j\hat{v}^{\alpha},g)^{q_{leaf_j}(0)}$。对于非叶子节点 ρ，其所有子节点 z 调用算法 Ver_{node}，并输出 F_z；设$\hat{s}_\rho$表示子节点集合 Z 的规模，集合存在，F_z 正常输出；否则，F_z 异常终止。

第二步　设

$\Delta_{\hat{s}_\rho,index(z)}=\prod_{l\in\{index(z):z\in\hat{s}_\rho\}-l/(index(z)-l)}$；系统计算

$$F_\rho=\prod_{z\in\hat{s}_\rho}F_z^{\Delta_{\hat{s}_\rho,index(z)}}=\prod_{z\in\hat{s}_\rho}e(A_j\hat{v}^{\alpha},g)^{q_z(0)\cdot\Delta_{\hat{s}_\rho,index(z)}}=\prod_{z\in\hat{s}_\rho}e(A_j\hat{v}^{\alpha},g)^{q_{parent}(index(z))\cdot\Delta_{\hat{s}_\rho,index(z)}}=e(A_j\hat{v}^{\alpha},g)^{q_\rho(index(0))}$$

Authority-Verify(σ,gpk,m,λ)算法初始化，系统选择签名 σ、群公钥 gpk、消息 m 和属性集 λ。系统验证签名 $F_{root}=e(\sigma_2,\omega),(\hat{u},\hat{v})=H(gpk,m,\lambda)$。

第三步　Authority 计算

$\overline{y_1}=\hat{u}^{T_\alpha}/\sigma_1$

$\overline{y_2}=e(\sigma_2,g)^{T_x}\cdot e(\hat{v},\hat{\mathbb{Q}})^{-T_\alpha}\cdot e(\hat{v},g)^{-T_y}\cdot(F_{root}/e(\hat{u},g))^C$

$\overline{y_3}=\sigma_3{}^{T_x}\hat{U}^{-T_y}$

如果 $C=H(gpk,m,\lambda,\sigma_1,\sigma_2,\overline{y_1},\overline{y_2},\overline{y_3})$，签名验证通过，Authority 为用户分发解密私钥。如果验证未通过，Authority-Revoke-User($spara,msk,i,\lambda$)算法初始化，系统选择公共参数、主私钥、用户身份 i 和属性集 λ；对于任意的 $i\in\lambda$，设定 λ 为空集，T_{ji} 中的 i 列加入撤销列表，撤销用户身份。

第四步　Authority-Keygen($spara,msk,\psi',\hat{\mathbb{Q}},\omega',gsk_{\omega'}$)算法初始化，系统选择 $\psi'\subseteq\psi$(且 $\psi'=\psi\cup(\mathbb{Q}-\psi)$)、公共参数 $spara$、主私钥 msk、$\hat{\mathbb{Q}}$、ω' 和 $gsk_{\omega'}$，输出用户解密密钥 SK。User-Decrypt($CT,spara,msk,i,SK$)算法初始化，系统选择密文 CT、公共参数 $spara$、主私钥 msk、用户身份 i 和解密密钥 SK。

第五步　定义递归算法 DecryptNode(CT,SK,x)，其中 $CT=\{\hat{\mathbb{Q}},\mathbb{A},c_0,c_1,c_2,c_3,c''\}$，$SK$ 关联一组属性 ω_j 和访问树 $\mathbb{A}$ 节点 x。设节点 x 有 $j=att(x)$，如果 $j\in\omega_j$，DecryptNode(CT,SK,x)$=\dfrac{e(D_j,C_0)}{e(\hat{D}_j,C_1)}\cdot\dfrac{e(T_{j,i},C_2)}{e(T_{j,i},C_3)}=e(g,g)^{q_x^{(0)}}$；如果 $j\notin\omega_j$，DecryptNode(CT,SK,x)异常退出。

第六步　设节点 x 的所有子节点 z，输出为 F_z；设 S_x 为所有子节点 z 的规模，系统计算

$$F_x=\prod_{z\in S_x}F_z^{\Delta_{j,s_x'}(0)}=\prod_{z\in S_x}(e(g,g)^{r q_z^{(0)}})^{\Delta_{j,s_x'}(0)}$$
$$=\prod_{z\in S_x}(e(g,g)^{r q_j^{(x)}})^{\Delta_{j,s_x'}(0)}=e(g,g)^{r q_x^{(0)}}$$

第七步　如果根节点为 R 的树 $\mathcal{T}$ 满足属性集 S，集合 A=DecryptNode(CT,SK,R)$=e(g,g)^{rq_R^{(0)}}=e(g,g)^{rs}$，解密 $C_0/(e(C_1,D)/A)=C_0/(e(\omega^s,g^{(\alpha+\gamma)/\beta}D)/e(g,g)^{rs})=m$。

4.2　安全分析

在标准模型下，基于属性的用户权限管理方案满足适应性选择消息攻击(IND-UAMBA-CCA2)。Owner 自定义属性树访问结构和多项式生成密文，Authority 无法更改属性树基本结构和节点集合；用户自定义多个随机数和基于属性集的私钥组件群签名消息，其它用户和 Authority 无法伪造群签名；攻击者无法连接签名会话过程，因此无法伪造第二个有效签名。如果任何多项式时间概率攻击者 $\mathcal{A}$ 在下列游戏中最多具备一个不可忽略的优势，基于属性的用户权限管理方案签名不可伪造。UAMBA 签名不可伪造证明如下。

系统建立　攻击者 $\mathcal{A}$ 向挑战者 $\mathcal{C}$ 发送一个属性树 Γ^*，$\mathcal{C}$ 运行 Setup 和 Authority-Keygen 算法，生成基于属性树 Γ^* 的群公钥 gpk^* 和成员私钥 gsk_i^*，并向 $\mathcal{A}$ 传递 gpk^* 和 gsk_i^*。

第一阶段　$\mathcal{C}$ 响应 $\mathcal{A}$ 的私钥、签名和撤销询问。

Authority-keygen-Query：当 $\mathcal{A}$ 询问身份 i^* 属性为 ω_i^* 的用户私钥 gsk_i^* 时，$\mathcal{C}$ 运行密钥生成算法，$\mathcal{C}$ 选择随机数 r^*、r_i^*，输入 ω_i^*、$spara^*$、$\hat{\mathbb{Q}}^*$ 和 msk^*，输出 $gsk_{\omega_i^*}^*=(\omega_i^*,D^*,D_l^*,\hat{D}_l^*,A_i^*,x_i^*,T_{i^*,1},\cdots,T_{i^*,n})$响应 $\mathcal{A}$。

User-Sign-Query：当 $\mathcal{A}$ 询问身份 i^* 满足 Γ^* 属性 ω_i^* 的用户签名 σ^* 时，$\mathcal{C}$ 运行用户签名算法，首先查找是否存在本地存储。如果不存在，$\mathcal{C}$ 执行密钥算法获得密钥对(gpk^*，$gsk_{\omega_i^*}^*$)，存储至本地数据库；$\mathcal{C}$ 选择随机数 ρ^*、λ_α^*、λ_x^* 和 λ_y^*，输入 $spara^*$、$\hat{\mathbb{Q}}^*$ 和 m^*，输出 $\sigma^*=(\hat{\mathbb{Q}}^*,\sigma_1^*,\sigma_2^*,\sigma_3^*,C^*,T_\alpha^*,T_x^*,T_y^*)$响应 $\mathcal{A}$。

Authority-Revoke-User-Query：当 $\mathcal{A}$ 询问身份 i^* 满足 Γ^* 属性 ω_i^* 的撤销用户时，$\mathcal{C}$ 运行撤销用户算法，输入 $spara^*$、msk^*、i^* 和 ω_i^*，输出一个新的 T_{j^*,i^*}^*、$gsk_{\omega_i^*}^*$ 响应 $\mathcal{A}$。

挑战阶段　$\mathcal{A}$ 提交 ω_i^*、m^*、两个身份 i_0^* 和 i_1^*，如果$(i_0,i_1)\neq(i_0^*,i_1^*)$，$\mathcal{C}$ 应答失败。否则，$\mathcal{C}$ 随机选择 $b\in(0,1)$，同样方法生成一个签名 σ_b 响应 $\mathcal{A}$。

第二阶段　和第一阶段相同类型的询问。

猜测阶段　$\mathcal{A}$ 提交一个 b'，如果 $b'=b$，那么 z 是随机的，否则 $z=U_2^{y+b}$。如果 z 是随机的且 $\mathrm{adv}(\mathcal{A})=|P_r[b'=b]-1/2|$，那么签名可以识别，$\mathcal{C}$ 以可忽略优势赢得了安全游戏。

4.3　性能分析

本文给出基于属性的用户权限管理方案与文献[23,30]在通信成本、存储开销和计算成本的比较分析。

4.3.1　通信成本

各系统中通信成本主要由密钥和签名长度产生，如表 1 所列。设 $|\mathbb{G}|$、$|\mathbb{G}_T|$ 表示群元素规模，$|n|$ 表示签名长度，Pr 表示签名和验证过程的双线性对运算，Sm 表示系统参数，Exp 表示指数运算。本文方案 Owner、Authority 和 Users 之间的通信成本来自于系统参数、主密钥、用户私钥和签名。Owner 和 Authority 之间的密钥通信成本主要是系统参数长度，Authority 和 Users 签名与验证贡献了主要的通信成本。本文方案中，签名与验证的通信成本主要与 Sm、Pr 和 Exp 相关；文献[23]主要是群签名验证的通信成本，主要与 Sm、Pr 和 Exp 相关；文献[30]主要是发布用户私钥的通信成本，与 Exp、Pr、$|\mathbb{G}_T|$、$|q|$ 相关。比较结果，本文方案通信成本低于文献[23,30]。

表 1　通信成本比较

通信成本	本文方案	方案[23]	方案[30]
Owner 和 Authority	1Sm	1Sm+1Pr	2Pr+2Exp
Authority 和 Users	1Sm+1Pr+1Exp	2Pr+2Exp	$\|\mathbb{G}_T\|\times\|q\|$

4.3.2　存储开销

各系统中每个实体存储开销如表 2 所列，$|q|$ 表示 z_p 元素规模，$|\mathbb{G}|$、$|\mathbb{G}_T|$ 表示群元素规模，n_a、n_u 表示系统用户属性数、用户总数，Sm 表示系统参数，$|n|$ 表示签名长度，$\mathbb{L}$ 表示密文关联的属性数。本文方案用户存储开销包含签名长度、群公钥和签名私钥，群公钥、签名私钥规模与 n_a 呈线性关系；Authority 存储开销包含系统参数、群公钥；Owner 主要存储开销是密文。文献[23] Authority 存储开销包含系统参数、主密钥和用户私钥；用户存储开销主要是签名和消息头。文献[30]中每个实体的存储开销主要与$|q|$、$|\mathbb{G}|$和$|\mathbb{G}_T|$相关。

表 2　存储开销比较

实体	本文方案	方案[23]	方案[30]
Owner	$(2+L\ n_a)\|q\|$	$\|G\|+2\|q\|$	$L\|G_T\|+Sm\|q\|$
Users	$(\|n\|+Sm)\|G\|$	$\|q\|\times\|G_T\|+n_a\|G\|$	$n_a\|G_T\|+Sm\|G\|$
Authority	$2Sm+\|G_T\|$	$2Sm+2\|G_T\|$	$2Sm+2\|G_T\|\times\|q\|$

4.3.3　计算成本

各系统中每个实体计算成本由签名与验证、加密与解密的哈希运算、指数运算和双线性对运算产生，如表 3 所列。设 $|q|$ 表示群的阶，$|G|$、$|G_T|$ 表示群元素规模，$|n|$ 表示签名长度，Pr 表示签名和验证过程的双线性对运算，Sm 表示系统参数，Exp 表示群上的指数运算。在双线性映射和标准模型下，基于属性的用户权限管理方案计算成本有较大改进；在指数运算、双线性对运算方面优于文献[23,30]方案。本文方案在 DBDH 困难性假设下，具有适应性选择消息攻击下存在签名不可伪造，系统计算成本优于文献[23,30]方案。

表 3　计算成本比较

指标	本文方案	方案[23]	方案[30]
签名算法	1Sm+1Exp	2Sm+1Pr+1Exp	2Pr+4Exp
验证算法	2Sm+1Pr	1Sm+2Pr+1Exp	1Sm+2Pr+2Exp
签名长度	$1\|n\|+1\|G_T\|$	$2\|n\|\times\|G_T\|$	$1\|q\|\times1\|G_T\|$
模型	标准	RO	RO

综合通信成本、存储开销和计算成本 3 个方面，本文方案系统综合性能优于[23,30]方案。

5　面向云计算的 CP-ABE 群签名用户权限管理认证方案

在线 PHR(Personal Health Records)服务[3]是典型的细粒度云环境数据访问控制服务系统，包含 3 个实体：用户(Users，包含患者家属 OF、医护人员 OD、研究人员 OR)、系统管理员(Authority)和患者(Owner)。Authority 负责为 Owner 分发加密密钥，为 Users 验证身份属性并分发解密密钥；Owner 加密数据并迁移至云服务器，Users 利用获得的解密密钥来解密密文。基于属性的用户权限管理方案实际应用场景认证应用的基本框架如图 2 所示，系统包含 4 个组件：Web Browser，Users，Authority 和 Cloud Server。Web Browser 代表 Users 与 Authority 通过在线交互完成认证。当 User 通过浏览器向 Authority 发出认证请求时，Authority 返回认证请求；当 User 收到认证请求，执行 User-Sign($\hat{\mathbb{Q}}$，gpk，m，gsk_ω)群签名算法输出签名 σ；Authority 执行 Authority-Verify(σ，gpk，m，λ)算法验证签名有效及不可伪造，身份认证通过；Authority 为 User 分发解密密钥。

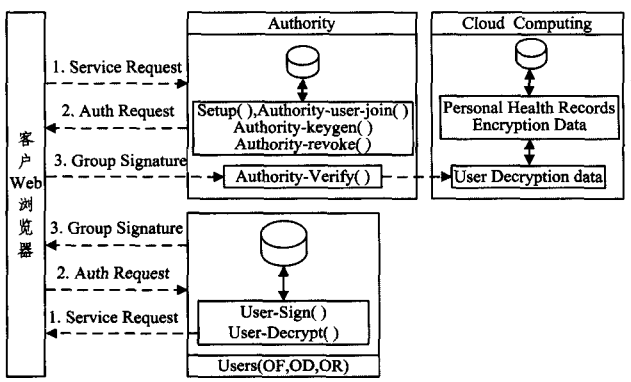

图 2　认证应用基本框架

结束语　用户权限分配是云计算安全的焦点，群属性集更新服务是云计算用户属性管理的服务之一。基于属性的 CP-ABE 群签名用户权限管理系统，以随机语言模型下的 CP-ABE 和群加入为基础，对标准模型下的群签名方案进行了相关扩展，融合了标准模型下的群签名撤销，解决了数据所有者重加密数据的中心瓶颈、共谋用户身份伪装和签名伪造问题。系统所有操作均在脱机状态下完成，用户在申请解密密钥服务之前消除了与可信第三方的交互通信；并通过群签名与验证的方法结合 Authority 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应用架构。基于属性的用户权限管理方案简化了 CP-ABE 的双线性对运算、指数运算次数，消除了用户属性存储负载，降低了群签名算法和验证算法的运算负载，但增加了系统参数数量和用户群私钥本地存储开销，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] Armbrust M, Fox A. Above the Clouds: A Berkeley View of Cloud Computing[R]. UC Berkeley Reliable Adaptive Distributed Systems Laboratory, 2009

[2] 李拴保，傅建明，连向磊. 植入城市计算综述[J]. 计算机科学，2013，40(3)：8-15

[3] Li M, Yu S C, et al. Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings [C]// Proc of Secure- Comm 2010. LNICST 50, 2010: 89-106

[4] Zhang H G, Li C L, et al. Evolutionary cryptography against multidimensional linear cryptanalysis [J]. Sci China Inf Sci, 2011, 54(12): 2565-2577

[5] Zhang H G, Li C L, et al. Capability of evolutionary cryptosystems against differential cryptanalysis [J]. Sci China Inf Sci, 2011, 54(10): 1991-2000

[6] Wang H Z, Zhang H G, et al. Extended multivariate public key crypto systems with secure encryption function[J]. Sci China Inf Sci, 2011, 54(6): 1161-1171

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

[8] 冯登国，张敏，等. 云计算安全研究[J]. 软件学报，2011，22(1)：71-83

[9] 沈昌祥，张焕国，等. 信息安全综述[J]. 中国科学 E 辑：信息科学，2007，37(2)：129-150

[10] Sahai A, Waters B, et al. Fuzzy identity-based encryption[C]// Proc of EUROCRYPT 2005. Springer, Heidelberg, 2005, 3494: 457-473

[11] Goyal V, Pandey O, et al. Attribute-Based encryption for fine-grained access control of encrypted data[C]// Proc of the 13th ACM Conference on Computer and Communication Security. 2006: 89-98

[12] Bethencourt J, Sahai A, et al. Ciphertext-Policy Attribute-Based Encryption[C]// Proc of IEEE Symposium on Security and Privacy. 2007: 321-334

(下转第 177 页)

利用哈希函数对源消息进行了变化，使用线性随机网络编码，对信源和信宿节点的编译码算法进行了变化，中间节点不需要改变编码方案。通过增加少量的计算复杂度（信源信宿节点）和舍弃少量的带宽，使整个网络达到了理想的安全要求。

参 考 文 献

[1] Ahlswede R, Cai N, Li S-Y R, et al. Network information flow [J]. IEEE Transactions on Information Theory, 2000, 46: 1204-1216

[2] Li S-Y R, Yeung R W, Cai N. Linear network coding[J]. IEEE Transactions on Information Theory, 2003, 49: 371-381

[3] Ho T, Medard M, Shi J, et al. On randomized network coding [C]// 41st Annual Allerton Conference on Communication Control and Computing. Oct. 2003

[4] Ho T, Leong B, Koetter R, et al. Toward a random operation of networks[J]. IEEE Transactions on Information Theory, submitted, 2004

[5] Cai N, Yeung R W. Secure network coding[C]// International Symposium on Information Theory (ISIT) 2002. Lausanne, Switzerland, 2002: 30-50

[6] Bhattad K, Narayanan K R. Weakly secure network coding [C]// Proc. 1st Workshop Netw. Coding Theory Appl, Apr. 2005

[7] Ho T. Networking from a network coding perspective [D]. MIT, 2004

[8] Jaggi S, Langberg M, Katei S. Resilient Network Coding in the Presence of Byzantine Adversaries [C]// 26th IEEE International Conference on Computer Communications. Anchorage: IEEE Press, 2012: 616-624

[9] Nutman L, Langberg M. Adversarial Models and Resilient Schemes for Network Coding [C]// IEEE Intl Symp Inf Theory. Toronto: IEEE Press, 2008: 171-175

[10] Cai N, Yeung R W. Network Coding and Error Correction [C]// IEEE Inform Theory Workshop. Bangalore: IEEE Press, 2002: 119-122

[11] Zhang Z. Network Error Correction Coding in Packetized Networks [C]// IEEE Information Theory Workshop Chengdu, ITW'06. IEEE Press, Chengdu, 2006: 433-437

[12] Zhang Z. Linear Network Error Correction Codes in Packet Networks [J]. IEEE Trans on Inf Theory, 2012, 54(1): 209-218

[13] 韦勇，连一峰. 基于日志审计与性能修正算法的网络安全态势评估模型[J]. 计算机学报，2009，32(4)：763-772

[14] Ho T, Leong B, Koetter R. Byzantine Modification Detection in Multicast Networks with Random Network Coding [J]. IEEE Transactions on Information Theory, 2012, 54(6): 2798-2830

[15] 周业军，李晖，马建峰. 一种防窃听的随机网络编码 [J]. 西安电子科技大学学报，2009，35(1)：696-701

[16] 武广柱，王劲林，齐卫宁. ARLNCStream：自适应随机网络编码流媒体系统[J]. 电子与信息学报，2008，30(1)：25-28

[17] 王汝言，楼芃雯，樊思龙，等. 容迟网络编码节点状态感知的数据转发策略[J]. 重庆邮电大学学报：自然科学版，2013，25(2)：215-220

(上接第 151 页)

[13] Pirretti M, Traynor P, et al. Secure attribute based systems [C]// Proc of the 13th ACM conference on Computer and Communication Security. 2006: 99-112

[14] Yu Shu-cheng, Wang Cong, et al. Attribute Based Data Sharing with Attribute Revocation[C]// Proc of ASIACCS. 2010: 261-270

[15] Wang Guo-jun, Liu Qin, et al. Hierarchical attribute-based encryption for fine-grained access control in cloud storage services [C]// Proc of CCS-2010. 2010: 735-737

[16] Yu Shu-cheng, Wang Cong, et al. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing [C]// Proc of INFOCOM. 2010: 15-19

[17] Wang Guo-jun, Liu Qin, et al. Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers[J]. Computers & Security, 2011, 30: 320-331

[18] Nuttapong A, Hideki I. Conjunctive Broadcast and Attribute-Based Encryption [M] // Pairing-Based Cryptograph-Pairing 2009. Springer Berlin Heidlberg, 2009: 248-265

[19] Niroshinie F, Seng W, et al. Mobile cloud computing: A survey [J]. Future Generation Computer Systems, 2013, 29: 84-106

[20] Ibraimi L, Petkovic M, et al. Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes [R]. Centre for Telematics and Information Technology, University of Twente, 2009

[21] Jae H S, Keita E. Efficient Delegation of Key Generation and Revocation Functionalities in Identity-Based Encryption[M]// Topics in Cryptology-CFRSA 2013. Springer Berlin Heidelberg, 2013: 345-358

[22] Yang Kan, Jia Xiao-hua, et al. Attribute-based Fine-Grained Access Control with Efficient Revocation in Cloud Storage Systems [C]// Proc of ASIA CCS. ACM, NY, 2013: 523-528

[23] Junbeom H, Dong K N. Attribute-based access control with efficient revocation in data outsourcing systems[J]. IEEE Transactions on Parallel and Distributed Systems, 2011, 22(7): 1214-1221

[24] Aggelos K, Moti Y. Group Signatures with Efficient Concurrent Join[C]// Proc of EUROCRYPT 2005. 2005: 198-214

[25] Dalia K. Attribute Based Group Signature with Revocation [R]. Cryptology ePrint archive: report 2007/241

[26] Dan B, Matt F. Identity-Based Encryption from the Weil Pairing [C]// Proc of CRYPTO 2001. 2001: 213-229

[27] Sujata M, Bansidhar M, et al. A secure electronic cash based on a certificateless group signcryption scheme[J]. Mathematical and Computer Modelling, 2013(58): 186-195

[28] Wang Chang-ji, Huang Jia-sen. Attribute-based Signcryption with Ciphertext-policy and Claim-predicate Mechanism[C]// Proc of Seventh International Conference on Computational Intelligence and Security. 2011: 905-909

[29] Keita E, Atsuko M, et al. Toward Dynamic Attribute-Based Signcryption[C]// Proc of ACISP 2011. 2011: 439-443

[30] Fan Chun-i, Wu Chien-nan, et al. Attribute-based strong designated-verifier signature scheme[J]. The Journal of Systems and Software, 2012(85): 944-959