云计算环境下基于属性的撤销方案

张光华[1,2] 刘会梦[2] 陈振国[3]
(西安电子科技大学综合业务网理论及关键技术国家重点实验室 西安 710071)[1]
(河北科技大学信息科学与工程学院 石家庄 050000)[2]
(华北科技学院河北省物联网数据采集与处理工程技术研究中心 河北 三河 065201)[3]

摘 要 针对云环境下密文策略属性基加密共享数据的访问权限撤销问题,提出了基于属性的撤销方案。方案中可信第三方从带有全局标识的用户属性集中查找满足密文访问结构的属性集,为该交集中的每个属性生成带有相同全局标识的密钥组件,通过组合密钥组件生成用户私钥。当发生撤销时,更新撤销用户属性的密钥组件并分发给拥有该属性的其他用户,同时生成对应的重加密密钥来对密文重加密。安全性分析和实验表明,本方案是选择明文攻击安全的,能有效实现属性的即时撤销,解决多授权结构密钥分发的同步问题。采用hash函数可使密文长度达到常数级,进一步减少资源开销,满足实际云环境中属性安全撤销的应用需求。

关键词 云环境,属性撤销,属性加密,单可信第三方,资源开销
中图法分类号 TP309.2 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.08.024

Attribute-based Revocation Scheme in Cloud Computing Environment

ZHANG Guang-hua[1,2] LIU Hui-meng[2] CHEN Zhen-guo[3]
(State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China)[1]
(College of Information Science and Engineering, Hebei University of Science and Technology, Shijiazhuang 050000, China)[2]
(Hebei Engineering Technology Research Center for IOT Data Acquisition & Processing, North China Institute of Science and Technology, Sanhe, Hebei 065201, China)[3]

Abstract Aiming at the problem of revoking the access rights of the ciphertexts policy attribute base encryption shared data in the cloud environment, the revocation scheme based on attribute was proposed. In the scheme, the trusted third party searches the attribute set satisfying the ciphertext access structure from the user attribute set with the global identity, generates the key component with the same global identity for each attribute in the intersection, and generates the user private key by combining the key components. When the revocation is occured, the scheme updates the key component which revokes the user attribute and distributes the component to other users who have the same attribute. At the same time, the corresponding re-encryption key is generated, and the ciphertext is re-encrypted in the cloud environment. The security analysis and experiments show that the scheme is safe to choose plaintext, which can effectively realize the real-time cancellation of attributes and solve the synchronization problem of multi-authorization structure key distribution. The hash function is used to make the ciphertext length constant, thus reducing the resource cost and meeting the application requirements of security in the real cloud environment.

Keywords Cloud environment, Attribute revocation, Attribute encryption, Single trusted third party, Resource overhead

为保证云计算环境下数据共享的安全性,Sahai等[1]于2005年提出了属性基加密(Attribute Based Encryption, ABE)方案,将属性标识与数据加密相关联,只有用户的属性集合满足访问结构时才有解密权限。与传统加密方案相比,ABE方案具有加密开销低、灵活性好、安全性高的特点,更能满足云计算环境中"一对多"的需求。为实现更加灵活的访问控制,Bethencourt等[2]提出了密文策略属性加密(Ciphertext Policy Attribute Based Encryption, CP-ABE)方案,将解密策略与密文相关联。CP-ABE方案的优点在于访问权限由数据拥有者控制,用户属性集满足访问结构时才能进行解密,能实现灵活度、细粒度更高的访问控制,更加适合云计算环境的应用场景。在实际云计算环境中,用户群是动态变化的,不断有用户注册进群和撤销出群,因此,提出一个支持属性安全撤销的CP-ABE方案对于保证云计算环境下数据的安全性具有重要意义。目前,CP-ABE撤销方案主要存在两方面的问题有:1)现有的撤销方法中属性撤销的即时性不高,多授权撤销

到稿日期:2017-06-13 返修日期:2017-09-09 本文受国家自然科学基金项目(61572255),中国博士后科学基金(2015M582622),河北省高等学校科学技术研究项目(ZD2018236,QN2017062),河北省科技计划支撑项目(15210338,15210703)资助。
张光华(1979-),男,博士,副教授,CCF会员,主要研究方向为信任管理、无线网络安全,E-mail:xian_software@163.com(通信作者);**刘会梦**(1991-),女,硕士,主要研究方向为网络安全;**陈振国**(1976-),男,博士,副教授,主要研究方向为网络安全、物联网。

方案存在如何为不同的第三方分配属性集使其负载均衡的问题；2）撤销时密文长度随属性数量的增加而不断增加，资源开销问题限制了撤销方案在云计算场景中的应用。

针对上述问题，本文提出云计算环境下基于属性的撤销方案，其能以较低的资源开销解决用户的撤销问题，保证用户撤销时数据的安全性。所提方法针对已有撤销方案的不足进行优化，以较低的计算开销实现属性的即时撤销，并且采用单可信第三方的方法减少撤销方案中对多授权机构的额外管理和通信开销，避免可信第三方之间出现负载均衡问题；通过 hash 函数实现属性空间到可计算群元素的无碰撞映射，使得密文长度随属性数量的增长呈常数级增长，以达到减少资源开销的目的。

本文第 1 节描述相关工作；第 2 节介绍相关背景知识；第 3 节提出云计算环境下基于属性的撤销方案；第 4 节分析并证明该方案的安全性；第 5 节给出仿真实验及其分析；最后总结全文。

1　相关工作

针对云计算环境下数据共享服务存在的用户撤销安全问题，众多研究者通过深入研究已提出一系列方案。目前，针对云计算环境下撤销问题的研究大致分为两个方面：1）撤销方法与属性的管理；2）资源开销。本文从这两个方面开展相关研究。

针对第一个研究点，根据撤销属性的影响范围对撤销方法进行分类，主要包括两种：用户部分属性撤销和用户撤销。用户部分属性撤销即仅对指定用户属性集的部分属性进行撤销，不影响拥有该属性的其他用户访问数据。文献[2]和文献[3]的方案实现了用户部分属性的撤销，通过设置属性的终止日期来限制密钥的使用，则授权机构的属性管理时间相对固定，无需一直在线。用户撤销即撤销用户的所有属性，不影响未撤销用户的使用。Hur 等[4]基于二叉树，通过向合法用户分发一个 KEK 二叉树，提出了支持用户部分属性撤销的 CP-ABE 方案，实现了属性的即时撤销；但此方案需要以较大的密钥维护开销。文献[5]的方案为属性添加了一个有效期，可信第三方周期性地进行版本更新以实现属性撤销；该方案中每个属性的有效期不同，为确保方案的可行性，授权机构必须一直保持在线状态，更新负荷较大。文献[6]和文献[7]的方案实现了间接的用户撤销，方案满足即时性的撤销；不过数据块的管理以及分割重组增加了开销，不支持用户进行多数据块访问。由上述分析可知，现有的撤销方法存在的问题在于：发生属性撤销时方案的即时性不高，且计算资源和通信资源的占用与用户数量和属性数量呈线性关系。根据撤销时属性管理机构的不同，将撤销方案分为单可信第三方和多可信第三方。多可信第三方即将第三方中心的管理权限分发给多个第三方，每个第三方中心管理互异的属性集并为用户分发私钥组件，最终通过组件合成密钥进行解密。Chase[8]首次提出了多可信第三方的 ABE 方案，在方案中添加全局 标识并通过结合用户密钥与全局标识的方法进行加密，通过聚合多个与其授权机构相关的密钥组件的方法进行解密。该方案中多个授权机构的管理依靠可信第三方，因此第三方的安全性限制了该方案的推广，撤销时系统开销较大。Lekwo 等[9]提出了无中心第三方的分布式 ABE 方案，该方案中第三方注册或撤销时，系统不需要重新初始化；但该方案由复杂的顺序双线性组合构造，需要较大的计算成本，并且该方案没有考虑属性的撤销问题。Yang 等[10]提出了一个解决多授权 CP-ABE 系统中属性撤销问题的方案，其中服务器不能获取密钥，系统安全性较高；但该方案在加解密效率方面的优势不明显，需进一步完善。Doshi 等[11]提出了一个定长密文的多可信第三方 CP-ABE 加密方案，其加解密效率较高；此方案中第三方需与属性授权机构共同分发私钥，使得密钥分发的管理成本明显增大。通过上述分析可知，多可信第三方授权虽然在密钥生成“去中心化”方面存在优势，但多可信第三方之间的属性集划分、负载均衡、通信资源开销以及可信第三方或无可信第三方对其的管理开销等方面仍然存在着诸多问题；而单属性授权机构方案存在着密钥托管、依赖可信第三方以及随着用户及其属性的增多计算负荷增大等问题。

资源开销问题是影响撤销方案实用性的一个重要因素，针对第二个研究点，在一般的密文策略撤销方案中，加解密开销与密文访问策略中属性的数量相关联，系统运算的资源开销随属性数量的增加而增加。在实际云计算环境中数据共享发生在多用户之间，资源开销成为了限制撤销方案应用的不可忽略的问题。Emura 等[12]首次提出了密文长度固定的属性撤销方案，基于(t,n)门限方法对属性公钥进行联合加密，从而使得密文长度不随属性数量的增加而改变。Herranz 等[13]采用(t,n)门限策略，制定适用于单调门限的访问结构。文献[14-15]提出了支持灵活撤销的门限访问策略，但是撤销的效率不高，加解密运算较复杂。通过上述分析可知，目前撤销方案存在的一个问题是密文长度随属性数量的增加而增加，且密文传输开销较大。

本文方案对已有撤销方案的不足进行优化，以较低的计算开销实现属性的即时撤销。对文献[16]中数据属主、云服务器、用户、认证机构以及多个属性授权机构 5 种角色的工作过程和算法原理进行深入分析，其中认证机构为完全可信机构，多个授权机构相互独立并且可以为非完全可信的。为了弥补其在负载均衡方面及计算开销方面的不足，本文方案将模型中的角色设计为数据属主、云服务器、用户以及可信第三方 4 种，并通过算法层面设计并实现了文献[16]方案中多个相互独立的授权结构以及认证机构的优化合并。本文方案将授权机构优化合并后，采用单可信第三方的方法减少了安全共享方案中对多授权机构的额外管理和通信开销，避免产生划分属性给不同的第三方使不同第三方之间负载均衡的计算开销。为了进一步减少第三方的计算和通信开销，方案采用 hash 函数来实现属性空间到可计算群元素的无碰撞映射，从而实现公开参数的群元素个数与 hash 函数的输出长度线性相关，而与属性空间的大小无关，进而减少了公开参数的数量，使得密文长度为常数级别，即当访问结构的属性增多时亦能使密文保持在相对固定的长度。

2　背景知识

2.1　双线性映射

定义 1（双线性映射[17]）　设置 G_1 和 G_2 为 2 个 P 阶加法循环群，G_T 为 P 阶乘法循环群，P 为素数，m 和 n 是 G_1 和 G_2 的生成元，Z_p 为模 P 的加法群。双线性对映射 $e:G_1\times G_2\rightarrow G_T$ 应具备以下性质。

1)双线性:若 $\forall m\in G_1$,$\forall n\in G_2$,$\forall a,b\in Z_p\times Z_p$,则 $e(m^a,n^b)=e(m,n)^{ab}$ 成立。

2)非退化性:对于 m 和 n,有 $e(m,n)\neq 1$,其中 1 为 G_T 的单位元。

3)可计算性:若 $\forall m\in G_1$,$\forall n\in G_2$,则可计算 $e(m,n)$。

2.2 (t,n)门限访问结构

定义 2((t,n)门限访问结构[18]) 每一个(t,n)门限都由一个阈值 t 和 n 个输入来描述,其中 $t\leqslant n$,并且每一个输入值只有 0/1 两种状态。若状态为 1 时输入数量大于或等于阈值 t,则该门限输出为 1,否则输出为 0[18]。另外,当阈值 $t=1$ 时,该门限为"OR";当阈值 $t=n$ 时,该门限为"AND"。在基于属性加密的方案中,系统门限阈值为 t,与用户身份相关联的属性集为 w,与密文相关联的属性集为 w'。如果 $|w\cap w'|\geqslant t$,那么 w 满足该访问结构,即用户可以对密文解密。因此,生成密文时,属性集被分为两类:一类是授权访问集合,用户的属性集满足 $|w\cap w'|\geqslant t$;另一类是非授权访问集合,用户的属性集满足 $|w\cap w'|<t$。图 1 中的 T 与本段中的 t 意义相同,均表示阈值。

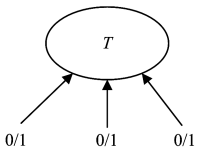


图 1 (t,n)门限访问结构图

Fig. 1 (t,n) threshold access structure

2.3 判定性 q-parallel DBHE 假设

定义 3(判定性 q-parallel DBHE 假设[19]) 根据安全参数选择一个阶为素数 P 的群 G,g 是 G 的生成元,选定随机值 $a,s\in Z_p$,则有敌手 $\vec{y}=g,g^s,g^a,\cdots,g^{a^q},g^{a^{q+2}},\cdots,g^{a^{2q}}$,$\forall 1\leqslant j\leqslant q,g^{s\cdot b_j},g^{a/b_j},\cdots,g^{a^q/b_j},g^{a^{q+2}/b_j},\cdots,g^{a^{2q}/b_j}$,$\forall 1\leqslant j,k\leqslant q,k\neq j,g^{a\cdot s\cdot b_k/b_j},\cdots,g^{(a^q\cdot s\cdot b_k/b_j)}$ 后,必须将 $e(g,g)^{a^{q+1}s}\in G_T$ 与 G_T 中的随机值区分开。

该算法在处理 G 中判定性 q-parallel DBHE 问题时输出最后猜想 $Z\in\{0,1\}$的优势为 ε,如果满足 $|\Pr[B(\vec{y},T=e(g,g)^{a^{q+1}s})=0]-\Pr[B(\vec{y},T=R)=0]|\geqslant\varepsilon$,则认为若在任何多项式时间内敌手都只有可忽略的优势攻破判定性 q-parallel DBHE 假设,那么判定性 q-parallel DBHE 假设成立。

2.4 CP-ABE 算法

定义 4 支持属性撤销的 CP-ABE 方案由 4 个环节组成[20]:$setup(k)$,$KeyGen(ID,\omega,mk,pk)$,$Encrypt(m,\tau,pk,R)$和 $Decrypt(c,sk_{\omega,ID},pk)$。

1)$setup(k)$:输入安全参数 k,输出主密钥 mk 和主公钥 pk。

2)$KeyGen(ID,\omega,mk,pk)$:输入主密钥 mk 和主公钥 pk、属性集合 ω、用户标识 ID,输出用户 ID 对应的属性私钥 $sk_{\omega,ID}$。

3)$Encrypt(m,\tau,pk,R)$:输入系统公钥 pk、消息 m、访问树 τ 及用户撤销列表 R,计算密文 c。

4)$Decrypt(c,sk_{\omega,ID},pk)$:输入用户私钥 $sk_{\omega,ID}$、密文 c、系统公钥 pk,当用户 ID 所拥有的与访问结构 τ 相关的未被撤销的属性集合满足访问树时,输出明文 m。

3 基于属性的撤销方案

3.1 总体方案

总体方案由 4 部分实体组成:数据属主、云服务器、可信第三方和用户。基于属性的撤销方案的框架如图 2 所示。

1)数据属主:提供共享数据源,选择系统参数对上传数据进行加密,并将密文上传至云端进行存储。

2)云服务器:提供大容量的存储环境,负责存储密文以及密文的重加密计算,具有"诚实且好奇"的特性。

3)可信第三方:负责管理数据属主和用户,可撤销指定用户的属性,生成重加密密钥,以及针对性地分发和更新密钥。

4)用户:共享数据的使用方,当其属性集满足访问结构设置时,获得解密密文的权限。

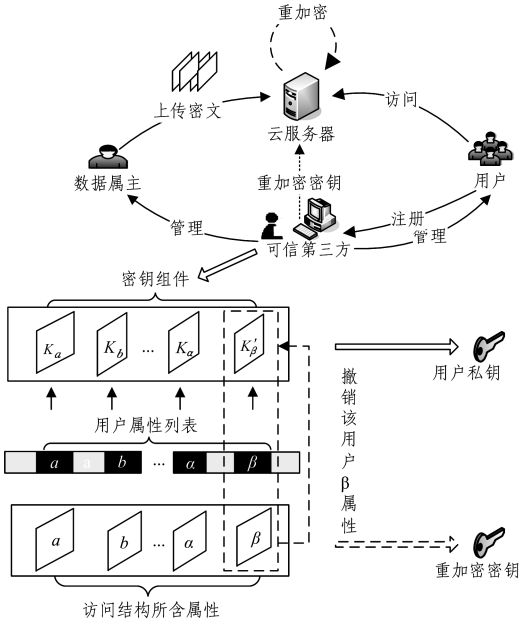


图 2 基于属性的撤销方案的框架

Fig. 2 Attribute-based revocation scheme framework

3.2 详述方案

首先对数据进行初始化,为每个授权用户生成唯一的全局标识并计算属性私钥;然后对上传数据进行加密,并将密文上传存储至云服务器;接下来通过可信第三方验证用户的合法性,并生成用户的唯一私钥;若用户属性集满足访问结构的设置,则可以解密密文以获得共享数据;当用户完成数据共享需要撤销时,可信第三方为撤销属性的私钥组成部分进行更新,使得撤销用户无法获得共享数据;最后对含有撤销属性的密文进行重加密,并保存至云服务器。该方案不仅充分利用了云环境的计算能力,还提高了数据的安全性,其具体过程分为如下 6 个部分。

1)初始化

$TTPSetup$:可信第三方 TTP 选择阶为素数 p 的两个循环群 G 和 G_T,$e:G\times G\rightarrow G_T$ 是一个双线性映射,$g\in G$ 是随机生成元,$H:\{0,1\}^*\rightarrow G$ 为一个哈希函数,U 是所有的属性集合,n 为属性集合中属性的数量,$n_i(1\leqslant i\leqslant n)$为每一个属性具有的属性值。$TTP$ 为每一个合法用户生成一个唯一的全局

标识 ID，为属性集中的每一个属性值选择随机值 $r_{i,j}, x_{i,j} \in Z_p^*$ $(1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n_i)$ 作为主密钥 MSK。结合数据属主发送的私钥 $SK_o = \{1/\gamma\}$ 计算出对应的属性公钥，如式(1)所示：

$$PK: \{\langle u_{i,j} = g^{-r_{i,j}^{\frac{1}{\gamma}}}, h_{i,j} = e(g,g)^{x_{i,j}^{\frac{1}{\gamma}}} \rangle \mid (1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n_i)\} \tag{1}$$

$OSetup(\gamma)$：随机选择 $\gamma \in Z_p^*$，输出数据属主的私钥 $SK_o = \{\frac{1}{\gamma}\}$，并将其通过安全信道发送给可信第三方 TTP。

2)加密

$Encrypt(PK, M, \tau)$：数据属主选择一个随机数 $s \in Z_p^*$，设置明文 $M \in G_T$ 的访问结构 $\tau = \{\tau_1, \cdots, \tau_m\}$ $(1 \leqslant m \leqslant n)$，其中 $\tau_i \in U$，根据 W 中的属性值 $v_{i,j}$ $(1 \leqslant i \leqslant m, j \in (1, n_i))$ 聚合公钥元素。密文 CT 可由式(2)计算得出：

$$CT = \langle C_1 = g^s, C_2 = (\prod_{v_{i,j} \in \tau} g^{-r_{i,j}^{\frac{1}{\gamma}}})^s, C_3 = M(\prod_{v_{i,j} \in \tau} e(g, g)^{x_{i,j}^{\frac{1}{\gamma}}})^s \rangle \tag{2}$$

$$\frac{C_3}{e(H(ID), C_2) \cdot e(SK_{\tau^*}^*, C_1)} = \frac{M(\prod_{v_{i,j} \in \tau} e(g,g)^{x_{i,j}^{\frac{1}{\gamma}}})^s}{e(H(ID), (\prod_{v_{i,j} \in \tau} g^{-r_{i,j}^{\frac{1}{\gamma}}})^s) \cdot e(\prod_{v_{i,j} \in \tau} g^{x_{i,j}^{\frac{1}{\gamma}}} H(ID)^{r_{i,j}^{\frac{1}{\gamma}}}, g^s)}$$

$$= \frac{M(\prod_{v_{i,j} \in \tau} e(g,g)^{x_{i,j}^{\frac{1}{\gamma}}})^s}{e(H(ID), (\prod_{v_{i,j} \in \tau} g^{-r_{i,j}^{\frac{1}{\gamma}}})^s) \cdot e(\prod_{v_{i,j} \in \tau} g^{x_{i,j}^{\frac{1}{\gamma}}}, g^s) \cdot e(\prod_{v_{i,j} \in \tau} H(ID)^{r_{i,j}^{\frac{1}{\gamma}}}, g^s)} = M \tag{4}$$

若用户的属性集 τ^* 不满足密文的访问结构 τ，则无法通过对应的属性 $v_{i,j}$ 计算出可解密密文的私钥 $SK_{\tau^*}^*$，进而无法解密密文。

5)撤销属性更新密钥

$ReGenKey(L, ID)$：假设撤销了用户 U_{ID} 的属性 $v'_{i,j} \in L$，其中 L 为撤销的属性集合。可信第三方 TTP 为撤销属性 $v'_{i,j}$ 选择新的主密钥 $MSK: r'_{i,j}, x'_{i,j} \in Z_p^*$ $(1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n_i)$，更新对应的公钥 $PK: \{\langle u'_{i,j} = g^{-r_{i,j}^{\frac{1}{\gamma}}}, h'_{i,j} = e(g,g)^{x_{i,j}^{\frac{1}{\gamma}}} \rangle \mid (1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n_i)\}$。

可信第三方 TTP 对其他拥有属性 $v'_{i,j}$ 的用户生成更新密钥 $UK_{i,ID} = \langle UK1_{i,ID} = (g^{\frac{1}{\gamma}})^{x'_{i,j} - x_{i,j} \frac{r'_{i,j}}{r_{i,j}}}, UK2_{i,ID} = \frac{r'_{i,j}}{r_{i,j}} \rangle$，更新其对应属性 $v'_{i,j}$ 的私钥组成部分，如式(5)所示：

$$K'_{i,ID} = (K_{i,ID})^{UK2_{i,ID}} \cdot UK1_{i,ID} = (g^{x_{i,j}^{\frac{1}{\gamma}}} \cdot H(ID)^{r_{i,j}^{\frac{1}{\gamma}}})^{\frac{r'_{i,j}}{r_{i,j}}} \cdot (g^{\frac{1}{\gamma}})^{x'_{i,j} - x_{i,j} \frac{r'_{i,j}}{r_{i,j}}} = g^{x'^{\frac{1}{\gamma}}_{i,j}} \cdot H(ID)^{r'^{\frac{1}{\gamma}}_{i,j}} \tag{5}$$

更新后的私钥为 $SK'_{\tau} = \prod_{v_{i,j} \in w} K_{i,ID}$，其中 $w \in \tau'$ 且 $w = \tau^*$，τ' 为撤销属性 $v'_{i,j}$ 后用户 U_{ID} 的属性集合，τ^* 为访问结构。

6)密文重加密

$ReEncrypt(CT, L)$：对于访问结构含有撤销属性 $v'_{i,j} \in L$ 的密文 CT，可信第三方 TTP 根据密文中的 C_1，由式(6)计算出密文的更新密钥：

$$\begin{aligned} CUK_{i,ID} &= (CUK1_{i,ID} = (C_1)^{\frac{1}{\gamma}(r_{i,j} - r'_{i,j})}, CUK2_{i,ID} = (g^{\frac{1}{\gamma}})^{x'_{i,j} - x_{i,j}}) \\ &= (CUK1_{i,ID} = g^{s \cdot \frac{1}{\gamma}(r_{i,j} - r'_{i,j})}, CUK2_{i,ID} = g^{\frac{1}{\gamma} \cdot (x'_{i,j} - x_{i,j})}) \end{aligned} \tag{6}$$

可信第三方将更新密钥通过安全通道发送给云服务器，使其对保存的密文进行重加密，以获得更新后的密文 $CT' = (C'_1, C'_2, C'_3)$，运算过程如式(7)－式(9)所示：

3)生成用户私钥

$UkeyGen(ID, \tau^*, MSK, SK_o)$：可信第三方 TTP 对用户的合法性进行验证。根据用户的全局标识 ID、用户含有的属性集 τ^*、TTP 生成的主密钥 MSK 和数据属主的私钥 SK_o，计算出该用户的私钥。用户的属性集为 $\tau^* = \{\tau_1^*, \cdots, \tau_u^*\}$ $(1 \leqslant u \leqslant n)$，其中 $\tau^* \in U$，根据用户的属性值 $v_{i,j}$ $(1 \leqslant i \leqslant u, j \in (1, n_i))$ 生成的用户私钥由式(3)计算得出：

$$SK_{\tau^*} = \langle \forall v_{i,j} \in L, K_{i,ID} = g^{x_{i,j}^{\frac{1}{\gamma}}} H(ID)^{r_{i,j}^{\frac{1}{\gamma}}} \rangle \tag{3}$$

4)解密

$Decry(ID, SK_{\tau^*}, CT)$：输入用户的全局标识 ID、对应用户的属性集 τ^* 的私钥 SK_{τ^*}。若用户的属性集 τ^* 满足密文的访问结构 τ，则结合用户相应的属性 $v_{i,j}$ 计算出解密私钥 $SK_{\tau^*}^* = \prod_{v_{i,j} \in \tau} K_{i,ID}$，通过该私钥解密密文获得明文 M，如式(4)所示：

$$C'_1 = C_1 = g^s \tag{7}$$

$$C'_2 = C_2 \cdot CUK1_{i,ID} = (\prod_{v_{i,j} \in \tau} g^{-r_{i,j}^{\frac{1}{\gamma}}})^s \cdot g^{s \cdot \frac{1}{\gamma}(r_{i,j} - r'_{i,j})} \tag{8}$$

$$C'_3 = C_3 \cdot e(C_1, CUK2_{i,ID}) = M \cdot (\prod_{v_{i,j} \in \tau} e(g,g)^{x_{i,j}^{\frac{1}{\gamma}}})^s \cdot e(g^s, g^{\frac{1}{\gamma} \cdot (x'_{i,j} - x_{i,j})}) \tag{9}$$

4　安全性证明

通过将授权机构组合并采用单可信第三方进行授权管理，可以减少系统的额外管理开销，解决了多可信第三方密钥分发的同步问题。此外，本文方案的密文为常数级别，密文长度不随访问结构中属性数量的变化而改变，可有效减少资源开销，适应云计算环境下大规模用户对数据共享的应用需求。本文设计的撤销方案的安全性分析具体可分为 5 个部分：1)在初始阶段进行系统初始化；2)阶段 1 返回私钥，根据不同属性结构的私钥发起攻击；3)挑战阶段根据反馈的私钥进行聚合，生成符合某个访问结构的密钥；4)阶段 2 重复阶段 1，每次使用一个不同的属性进行数据访问；5)最后在猜测阶段估计攻击成功的难度，即假设攻击成功，估计出系统所需的运算量。

定理 1　如果任意概率多项式时间的敌手在判断性 q-DBHE 游戏中的优势是可忽略的，那么数据安全共享机制是选择明文安全的。

在攻击者与挑战者游戏中，假设攻击者 A 攻破数据安全共享机制的优势为 ε，且密文的访问结构为 $\tau^* = \{\tau_1^*, \cdots, \tau_m^*\}$，那么可以构造一个能以 ε 的优势攻破判定性 q-DBHE 问题的模拟器 B。模拟器 B 挑战判定性 q-DBHE 问题 $(g, h, g^{\alpha}, g^{\alpha^2}, \cdots, g^{\alpha^q}, g^{\alpha^{q+2}}, \cdots, g^{\alpha^{2q}}, T)$，其中 $q = n \cdot n_i$，n_i 为属性集合的数量，$T = e(g_{q+1}, h)$ 或者随机选择 $T \in G_T$。模拟器 B 扮演挑战者角色，在初始阶段模拟器 B 为属性值 $v_{i,j}$ 构造公钥组件，其与攻击者 A 进行如下游戏。

初始阶段：模拟器 B 随机选择 $\gamma\in Z_p^*$，$r_{k,j},x_{k,j}\in Z_p^*$（$1\leqslant i\leqslant n,1\leqslant j\leqslant n_k$），$n$ 为属性集合中包含属性的数量，$n_k(1\leqslant i\leqslant n)$为每一个属性所具有的属性值。随机选择 $w^*\in\{1,2,\cdots,m\}$，$I^*\in\{1,2,\cdots,m\}$，$w\in I^*$，对于密文访问结构中的属性值 v_{i_w}，随机选择 $r_{i_w},y_{i_w}\in Z_p^*$，具体过程如下。

1）当 $i=w-\{w^*\}$ 时，对属性 $v_{i,j}$ 计算的公钥组成部分 $(u_{i,j},h_{i,j})$ 为：若 $v_{i,j}=\tau_i^*$，则 $(u_{i,j},h_{i,j})=(g^{r_{i_w}\frac{1}{\gamma}}g_{q+1-i_w}^{-1},e(g,g)^{a_{i_w}\frac{1}{\gamma}})$；若 $v_{i,j}\neq\tau_i^*$，则 $(u_{i,j},h_{i,j})=(g^{r_{i_w}\frac{1}{\gamma}},e(g,g)^{x_{i,j}\frac{1}{\gamma}})$。

2）当 $i=w=w^*$ 时，对属性 $v_{i,j}$ 计算的公钥组成部分 $(u_{i,j},h_{i,j})$ 为：若 $v_{i,j}=\tau_i^*$，则 $(u_{i,j},h_{i,j})=(g^{r_{i_w}\frac{1}{\gamma}}(\prod_{k\in I^*}-\{w^*\}g_{q+1-i_k}),e(g,g)^{a_{i_{w^*}}\frac{1}{\gamma}}e(g,g)^{\alpha^{q+1}})$；若 $v_{i,j}\neq\tau_i^*$，则 $(u_{i,j},h_{i,j})=(g^{-r_{i,j}},e(g,g)^{x_{i,j}\frac{1}{\gamma}})$。

3）当 $i\notin I^*$ 时，对属性 $v_{i,j}$ 计算的公钥组成部分为 $(u_{i,j},h_{i,j})=(g^{-r_{i,j}\frac{1}{\gamma}},e(g,g)^{x_{i,j}\frac{1}{\gamma}})$。

阶段 1　假设密文的访问结构 τ^* 只有一个属性 $i_{\acute{w}}$，攻击者 A 的属性值不满足该访问结构，即 $v_{\acute{w},j}\neq\tau_{\acute{w}}^*$，则攻击者 A 向模拟器 B 提交属性集合 $\tau\subseteq U$ 和系统全局标识 ID 查询私钥，同时模拟器 B 构建随机语言模型。若攻击者 A 提交的系统全局标识 ID 已经被查询过，则 $H(ID)$会被记录，此时模拟器 B 只需返回相应的值；若系统全局标识 ID 没有被查询过，则模拟器 B 为其随机选择 $s\in Z_p^*$，令 $H(ID)=g_{i'_w}g^s$。模拟器 B 计算出属性值 $v_{\acute{w},j}$ 对应的私钥组成部分为 $K_{\acute{w},j}=g^{x_{\acute{w},j}}(g_{i_{\acute{w}}},g^s)^{r_{\acute{w}j}}$，并将属性集 τ 的私钥 $SK=\langle\forall v_{\acute{w},j}\in L,K_{\acute{w},j}\rangle$ 返还给攻击者 A。当 $i\neq\acute{w}$ 时，对私钥 $K_{i,j}$ 的计算分为如下 3 步。

1）当 $i_k\in(\tau^*-\{i_{w^*}\})$，$k=i$ 时，$K_{i,j}=K_{i_k}=g^{a_{i_k}\frac{1}{\gamma}}(g_{i_w})^{r_{i_k}\frac{1}{\gamma}}g_{q+1-i_k+i_w}(u_{i_k})^{-s}$；

2）当 $i_k=i_{w^*}$，$k=i$ 时，$K_{i,j}=K_{i_{w^*}}=g^{a_{i_{w^*}}\frac{1}{\gamma}}(g_{i_w})^{-w^*\frac{1}{\gamma}}(\prod_{k\in I^*-\{w^*\}}^{i_k\neq i_w}g_{q+1-i_k+i_w}^{-1})(u_{i_k})^{-s}$；

3）当 $v_{k,j}\notin\tau^*$，$k=i$ 时，$K_{i,j}=K_{k,j}=g^{x_{k,j}\frac{1}{\gamma}}(g_{i'_w},g^z)^{r_{k,j}\frac{1}{\gamma}}$。

挑战阶段：攻击者 A 对加密公钥 $\langle u,h\rangle$ 进行聚合，其中，$u=u_{i_w}\prod_{k\in I^*-\{w^*\}}u_{i_k}=\prod_{j\in\{1,\cdots,m\}}g^{r_{i_j}\frac{1}{\gamma}}$，$h=u_{i_{w^*}}\prod_{k\in I^*-\{w^*\}}u_{i_k}=\prod_{j\in\{1,\cdots,m\}}e(g,g)^{a_{i_j}\frac{1}{\gamma}+\alpha^{q+1}}$，提交两个相同长度的消息 M_0 和 M_1，模拟器 B 以掷硬币的方式选择 $\delta\in\{0,1\}$，计算出系统的挑战密文 $CT^*=(W^*,C_1^*=g,C_2^*=\prod_{j\in\{1,\cdots,m\}}g^{r_{i_j}\frac{1}{\gamma}},C_3^*=M_\delta\cdot T\cdot\prod_{j\in\{1,\cdots,m\}}e(g,g)^{a_{i_j}\frac{1}{\gamma}})$。若 T 值为 $e(g^{\alpha^{q+1}},g)$，则挑战密文是对 M_δ 的有效加密；若 T 值为 G_T 上的随机数，则攻击者 A 无法识别出 δ 与挑战密文 CT^* 之间的关系。

阶段 2　重复阶段 1 的工作，攻击者 A 使用一个不同的属性继续进行私钥查询，模拟器 B 返回查询结果。

猜测阶段：攻击者 A 对 δ 猜测一个值 $\acute{\delta}$，若 $\delta\neq\acute{\delta}$，则模拟器 B 在 q-BDHE 游戏中输出 0，猜测 T 是 G_T 上的随机值 S，则有 $\Pr[B(g,h,g^\alpha,g^{\alpha^2},\cdots,g^{\alpha^q},g^{\alpha^{q+2}},\cdots,g^{\alpha^{2q}},S)=1]=\frac{1}{2}$；若 $\delta=\acute{\delta}$，则输出 1，猜测 $T=e(g^{\alpha^{q+1}},g)$，CT^* 是有效密文，则有 $\Pr[B(g,h,g^\alpha,g^{\alpha^2},\cdots,g^{\alpha^q},g^{\alpha^{q+2}},\cdots,g^{\alpha^{2q}},e(g^{\alpha^{q+1}},g))=1]=\frac{1}{2}+\varepsilon$。

综上所述，模拟器 B 以不可忽略的优势 ε 赢得判定性 q-BDHE 游戏，证明了本方案可保证云计算环境下数据共享过程是选择明文安全的，可有效防止非授权用户的攻击行为，从而实现用户的安全撤销。

5　实验仿真及性能分析

5.1　实验环境

本节对云计算环境下基于属性的撤销方案进行仿真。硬件配置为：Intel Core i3-3120 M 2.50 GHz，内存为 4.00 GB RAM，Win7-64。软件平台为 Eclipse4.3.0，代码库为 jPBC 2.0.0（Java Pairing-Based Cryptography Library），使用 jPBC 大数库实现双线性对运算、密码学相关运算以及加密执行时间测试等功能。数据来源为搜狗输入法用户的常用字词数据库，该数据主要以字符串形式进行存储。

5.2　仿真实现

本方案的实现基于 jPBC 代码库，对于方案中的数据属主、云服务器、可信第三方和用户 4 类角色，分别采用 4 个进程进行模拟，角色之间的通信通过 Socket 协议实现，仿真的实现流程如图 3 所示。

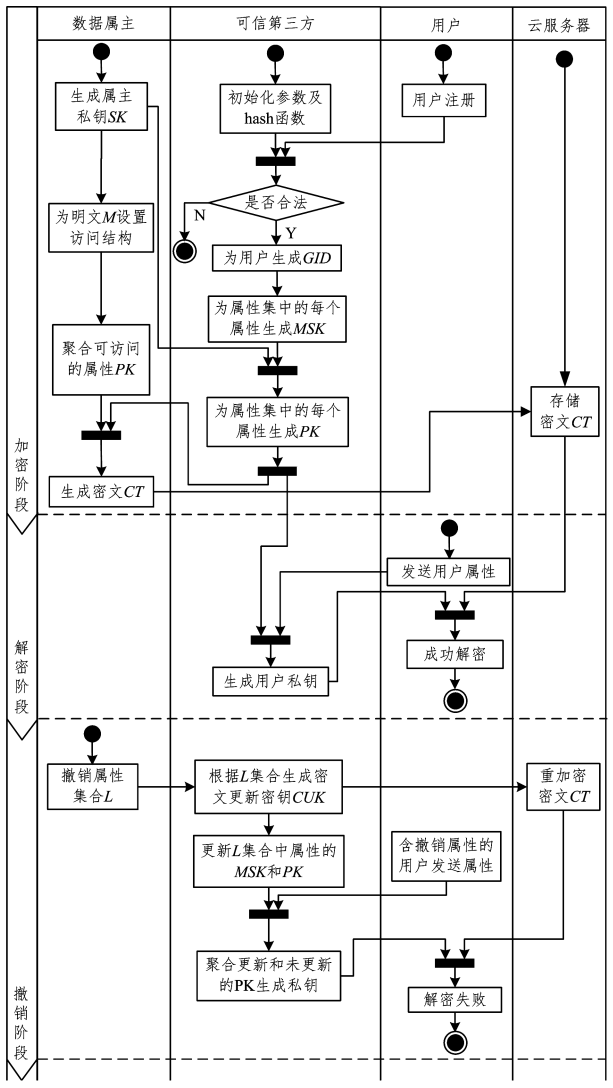


图 3　方案的实现流程图

Fig. 3　Program implementation process

图 3 分为加密阶段、解密阶段以及撤销阶段 3 个部分，对数据属主、云服务器、可信第三方以及用户 4 个仿真角色的交

互过程进行描述。根据用户角色的特征，可将其分为两类：一类是获得授权且可解密密文的用户；另一类是已撤销属性并且无法解密的用户。

5.3　性能分析

本文针对密文策略属性基加密方案中共享数据的访问权限撤销问题，提出属性撤销方案。方案中可信第三方生成带有相同全局标识的密钥组件，通过组合密钥组件生成用户私钥，有效地实现了属性的即时撤销，同时解决了多授权结构密钥分发同步的问题。当发生撤销时，更新撤销用户属性的密钥组件并分发给拥有该属性的其他用户，生成对应的重加密密钥，在云环境中对密文重加密，由于密文长度为常数级，因此进一步减少了资源开销。下面针对本文所提方案分别给出理论分析和实验仿真，以证明其有效性。

5.3.1　理论分析

本节将从属性撤销即时性、授权中心数量、安全性假设、访问策略、密文长度以及解密开销等方面将本文方案与其他方案进行对比，结果如表 1 所列。在解密开销部分，t 表示访问策略中的属性个数，k 表示方案中用户所拥有的属性个数，P 表示双线性配对操作。文献[2]方案的解密算法的复杂度为 $O(2kP+P)$，其计算开销主要取决于用户拥有的属性个数 k；文献[9]方案的解密算法的复杂度为 $O(2tP)$，其主要开销与访问策略中的属性个数 t 相关；文献[16]方案的解密复杂度及本方案的解密复杂度均为 $O(2P)$，解密的开销主要为常数级的双线性运算。

表 1　各方案性能的比较

Table 1　Performance comparison of each scheme

方案	撤销机制	授权中心数量	安全性假设	访问策略	密文长度	解密开销
文献[2]方案	周期撤销	单授权	group model	选择明文攻击安全	非常数级	$O(2kP+P)$
文献[9]方案	即时撤销	多授权	非标准假设	LSSS	非常数级	$O(2tP)$
文献[16]方案	即时撤销	多授权	q-BDHE	LSSS	常数级	$O(2P)$
本文方案	即时撤销	单授权	q-BDHE	选择明文攻击安全	常数级	$O(2P)$

综合表 1 中所述因素，本文方案的性能是最优的。从撤销机制方面来看，文献[2]方案不支持属性即时撤销，无法实现属性的灵活撤销。从授权中心数量方面来看，文献[9]和文献[16]均为多授权方案，需要解决给不同授权机构分发密钥的同步问题以及不同授权机构之间负载均衡的问题。从安全性假设及访问策略方面来看，文献[9]方案采用 LSSS 访问策略，满足非标准的安全性假设，其应用场景有限。从密文长度和解密开销方面来看，文献[2]方案和文献[9]方案的密文长度、解密开销均与系统中的属性总个数呈线性关系，计算开销随系统中属性数量的增加而增加，不适用于用户规模较大的应用场景。本文方案对属性撤销的即时性进行优化，采用单授权方式避免出现密钥分发的同步问题，满足了 q-BDHE 安全性假设和选择明文攻击安全的访问策略；同时，其采用 hash 函数实现属性空间到可计算群元素的无碰撞映射，使得密文长度为常数级，满足了大规模用户进行数据共享在计算开销方面的要求。通过上述理论分析可知，本文方案在数据安全性和资源消耗方面均实现了性能优化，兼顾了安全性与实用性。

5.3.2　实验仿真

本节将本方案与 Hur 方案、文献[16]方案进行了比较测试，对加密开销、解密开销以及重加密开销 3 个方面的仿真结果进行分析，以证明本文方案的性能。对方案的加密开销进行仿真的结果如图 4 所示。

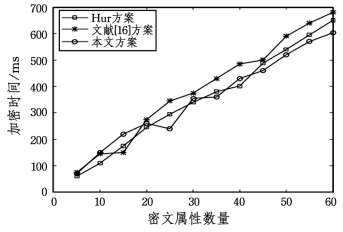
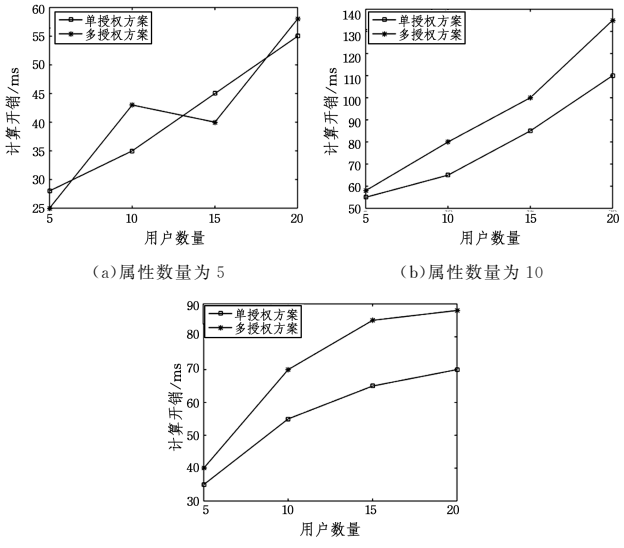


图 4　加密开销的对比

Fig. 4　Comparison of encryption overhead

图 5 给出了撤销属性数量为 5，10，15 时，单授权与多授权机构在密钥分发开销方面的仿真结果。由于每次仿真 IO 流、输入、输出等存在硬件差异，因此采用多次实验求期望值的方式得出结果。分析图 4 可知，系统加密时间与属性数量相关联并呈线性关系，加密时间随着用户属性数量的增加而增加。当属性数量较少时，本文方案相比其他方案在加密开销方面并无突出优势；当系统中用户属性数量较多时，本文方案在加密开销方面的优势明显，有效降低了系统的加密消耗，适用于云计算环境下大规模用户的应用场景。



(a)属性数量为 5　　(b)属性数量为 10

(c)属性数量为 15

图 5　密钥分发开销的对比

Fig. 5　Comparison of key distribution overhead

分析图 5 可知，随着属性数量的增加，多授权机构面临密钥分发同步问题的额外管理以及如何划分属性给不同的授权机构使不同的授权机构之间负载均衡的计算开销问题，通信开销较大；而单授权机构密钥分发避免了上述问题，所需的通信开销较小。图 5 表明，相较于多授权机构，单授权机构在密钥分发时产生的计算负荷更小，密钥分发效率更优。

解密开销的仿真结果如图 6 所示。在解密过程中，主要的计算开销是系统中每个用户属性对应节点的解密操作，本方案的解密开销主要为群上的乘除法运算，减少了计算开销

较大的双线性运算。与 Hur 方案和文献[16]方案相比，本文方案的解密开销曲线整体变化较平稳，增长幅度相对较小，随用户属性数量的增加优势愈发明显；并且当属性数量增至 60 时，解密时间在 260ms 左右，满足实际应用场景的需求。

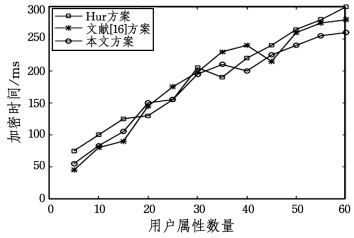


图 6 解密开销的对比

Fig. 6 Comparison of decrypt overhead

重加密开销的仿真结果如图 7 所示。仿真过程中假定撤销属性数量为固定值，图 7 中重加密开销随密文属性数量的增加而增加。当密文属性数量为 20 时，加密开销约为 90 ms；当属性数量为 40 时，开销约为 160 ms，重加密开销曲线变化较平稳。仿真结果说明：在本文方案中，当授权用户撤销后，系统仅对撤销用户的撤销属性密钥组件进行更新，对未撤销属性不进行重加密，从而提高了撤销效率，降低了重加密开销。

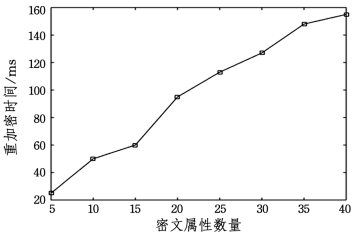


图 7 重加密开销

Fig. 7 Re-encryption overhead

结束语 针对云环境下密文策略属性基加密共享数据的访问权限撤销问题，提出了用户部分属性的撤销方案，并证明了本文方案在判定性假设下是选择明文攻击安全的。本文方案可有效实现属性的即时撤销，解决多授权结构密钥分发的同步问题。同时，采用 hash 函数实现属性空间到可计算群元素的无碰撞映射，使得密文长度为常数级，从而进一步减少了资源开销，满足实际云环境中属性安全撤销的应用需求。本文方案采用单授权方式进行密钥分发，一方面避免了不同授权机构分发密钥的同步问题以及不同授权机构间负载均衡的问题，另一方面使得授权机构的安全性问题显得越发重要。进一步提高授权机构的安全性，是下一步工作需要解决的问题。

参 考 文 献

[1] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]// International Confernece on Theory & Applications of Cryptographic Techniques. 2005: 457-473.

[2] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[J]. IEEE Symposium on Security & Privacy, 2007, 2008(4): 321-334.

[3] LIANG X H, LU R X, LIN X D, et al. Ciphertext Policy Attribute Based Encryption with Efficient Revocation[R]. Waterloo: University of Waterloo, 2010.

[4] HUR J, NOH D K. Attribute-based access control with efficient revocation in data outsourcing systems[J]. IEEE Transactions on Parallel and Distributed Systems, 2011, 22(7): 1214-1221.

[5] YU S, WANG C, REN K, et al. Achieving secure, scalable, and fine-grained data access control in cloud computing[C]// IEEE INFOCOM 2010 Proceedings. 2010: 1-9.

[6] CHEN Y, WANG Z Y, MA J, et al. Efficient revocation in cipher-text-policy attribute-based encryption based cryptographic cloud storage[J]. Journal of Zhejiang University-Science C, 2013, 14(2): 85-97.

[7] YAN X X, TANG Y L. Attribute－based encryption scheme with efficient revocation in data outsourcing systems[J]. Journal on Communications, 2015, 36(10): 92-100. (in Chinese)
闫玺玺，汤永利. 数据外包环境下一种支持撤销的属性基加密方案[J]. 通信学报，2015，36(10)：92-100.

[8] CHASE M. Multi-authority attribute based encryption [M]// Theory of Cryptography. Springer Berlin Heidelberg, 2007: 515-534.

[9] LEWKO A, WATERS B. Decentralizing attribute-based encryption[M]// Advances in Cryptology-EUROCRYPT 2011. Springer Berlin Heidelberg, 2011: 568-588.

[10] YANG K, JIA X. Attributed-based access control for multi-authority systems in cloud storage[C]// 2012 IEEE 32nd International Conference on Distributed Computing Systems (ICDCS). IEEE, 2012: 536-545.

[11] DOSHI N, JINWALA D. Constant ciphertext length in multiauthority ciphertext policy attribute based encryption[C]// 2011 2nd International Conference on Computer and Communication Technology (ICCCT). IEEE, 2011: 451-456.

[12] EMURA K, MIYAJI A, NOMURA A, et al. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length[M]// Information Security Practice and Experience. Springer Berlin Heidelberg, 2009: 13-23.

[13] HERRANZ J, LAGUILLAUMIE F, RÀFOLS C. Constant size ciphertexts in threshold attribute-based encryption[M]// Public Key Cryptography-PKC 2010. Springer Berlin Heidelberg, 2010: 19-34.

[14] GE A, ZHANG R, CHEN C, et al. Threshold ciphertext policy attribute-based encryption with constant size ciphertexts[C]// Australasian Conference on Information Security and Privacy. 2012: 336-349.

[15] ATTRAPADUNG N, HERRANZ J, LAGUILLAUMIE F, et al. Attribute-based encryption schemes with constant-size ciphertexts[J]. Theoretical Computer Science, 2012, 422(3): 15-38.

[16] CHEN Y, SONG L, YANG G. Attribute-Based Access Control for Multi-Authority Systems with Constant Size Ciphertext in Cloud Computing[J]. China Communications, 2016, 13(2): 146-162.

[17] SHAMIR A. Identity-based cryptosystems and signature schemes [C]// Proceedings of CRYPTO 84 on Advances in Cryptology. Berlin, 1985: 47-53.

[18] 单忆南. 基于属性的加密算法[D]. 上海：上海交通大学，2009.

[19] GENTRY C, PEIKERT C, VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions[C]// Proceeings of the 14th Annual ACM Symposium on Theory of Computing. 2008: 197-206.

[20] YAN X X, MENG H. Ciphertext policy attribute-based encryption scheme supporting direct revocation[J]. Journal on Communications, 2016, 37(5): 44-50. (in Chinese)
闫玺玺，孟慧. 支持直接撤销的密文策略属性基加密方案[J]. 通信学报，2016，37(5)：44-50.