云存储环境下支持策略变更的CP-ABE方案

熊安萍[1,2] 许春香[1] 冯 浩[2]
(电子科技大学计算机科学与工程学院 成都 610054)[1]
(重庆邮电大学计算机科学与技术学院 重庆 400065)[2]

摘 要 近年来,CP-ABE作为适用于云存储环境的访问控制机制,成为研究热点。由于现有的基于CP-ABE的访问控制方案在云存储环境下不支持系统属性灵活变更,利用云存储服务提供者的存储及计算资源优势,基于AB-ACER方案提出了支持系统属性灵活撤销及恢复的云存储访问控制方案。该方案通过引入虚拟属性来支持云存储环境下访问策略属性的撤销及恢复,且仅由存储服务提供者进行少量的重加密计算。安全及性能分析表明,该方案不仅支持数据属主访问策略的灵活变更,还保持了原有方案的安全性及细粒度访问控制,同时大大降低了数据属主的计算开销。

关键词 云存储,CP-ABE,系统属性变更,虚拟属性,访问控制
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.1.043

CP-ABE Scheme with Supporting Policy Elastic Updating in Cloud Storage Environment

XIONG An-ping[1,2] XU Chun-xiang[1] FENG Hao[2]
(School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China)[1]
(College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)[2]

Abstract In recent years, CP-ABE has been researched extensively as an access control mechanism in cloud storage environment. Because existing access control schemes based on CP-ABE can not support the elastic update with the system properties in cloud storage environment, this paper used the cloud storage service provider's(CSP's) storage and computing resources advantages, and proposed a cloud storage access control scheme which supports the system attributes revocation or recovery based on the attribute-based access control with efficient revocation(AB-ACER) scheme. The scheme introduces virtual attributes for the access control tree, and when system attributes have been revoked or recovered, CSP only provides small re-encryption computation. Security analysis and performance analysis show that the proposed scheme not only supports a changeable access control policy for data owner(DO), but also ensures the confidentiality of data and the fine-grained access control, and reduces a large number of encryption calculation works for DO.

Keywords Cloud storage, CP-ABE, System attribute update, Virtual attribute, Access control

1 引言

云存储作为一种基本服务得到了业界的广泛认同,越来越多的企事业单位或个人通过云存储服务保留各类数据信息。然而,网络时代的数据信息内涵非常丰富,往往隐含企业的商业秘密或涉及个人隐私,而提供存储服务的第三方往往是独立的运营管理机构或组织,并不完全值得信赖,诸多云存储安全事件[1-3]阻碍了云存储服务的广泛应用。

基于属性的加密(Attribute-Based Encryption)方案在业界已开展了大量研究,主要分为密钥策略KP-ABE(key-policy ABE)[4]与密文策略CP-ABE(ciphertext-policy ABE)[5]两种访问方案。CP-ABE可以由加密者即数据的拥有者定义自己的访问策略,更适用于云存储环境下实施共享数据的访问控制,因此得到了业界的广泛关注。

当前,大多数CP-ABE方案基于Decisional Bilinear Diffie-Hellman Problem(DBDH)问题构造,方案研究大都集中在两个方面:一是如何在减少数据属主开销的基础上支持可变策略的访问控制,即属性权限撤销问题;二是如何利用云计算环境强大的计算和存储能力来实现细粒度的、灵活的访问控制,包括支持用户属性的灵活变更。针对前者,本文基于现有的灵活细粒度访问控制方案[6-8],进一步提出了一个既能够减少数据属主计算开销,又能高效实现灵活访问控制的云存储访问控制方案。该方案通过算法构造,让云存储服务提供者利用其自身资源优势[9]进行密文与密钥密文的重加密工作,从而实现灵活的访问控制。

2 相关工作

近年来,针对基于属性的密文策略访问控制方案中用户属性撤销的研究成果较多。Bethencourt等人在文献[10]中首次提出CP-ABE方案,并在IBE数值系统属性撤销机制的启发下利用"AND"和"OR"门来实现数值比较方法,进行系统属性撤销。Pirretti等人在文献[11]中通过可信第三方维

到稿日期:2015-03-05 返修日期:2015-04-06 本文受国家自然科学基金项目(61350203),重庆市教委科学技术研究项目(KJ1400414)资助。
熊安萍(1970—),女,博士生,主要研究方向为信息安全、云计算,E-mail:xiongap@cqupt.edu.cn;许春香(1966—),女,博士,教授,主要研究方向为信息安全、密码学;冯 浩(1992—),女,硕士生,主要研究方向为云存储安全技术。

护一个被撤销的属性列表，定时更新被撤销属性列表中的用户私钥。针对用户被废止的属性，文献[12]通过定时密钥更新机制实现每个属性的自我撤销。这些方案的共同之处在于密钥的更新不随着属性的改变立即进行，且撤销机制往往是粗粒度的。Yu S 等[13,14]提出基于 CP-ABE 的资源共享方案中，系统属性撤销时需要同时更新系统的公开参数和用户的私钥来完成即时性的权限撤销，方案密钥更新代价较大，访问控制不灵活。文献[6]提出了一个细粒度的支持用户属性撤销机制的密文访问控制方案(Attribute-Based Access Control with Efficient Revocation，AB-ACER)，AB-ACER 对访问结构中每个属性生成一个重加密密钥，通过基于属性的重加密实现灵活访问控制，相比传统的 CP-ABE 方案，其在安全性和可扩展性方面都具有很大优势，但在策略变更时，DO 需要重新做一次加密，开销大，访问控制不灵活。

以上分析表明，现有基于 CP-ABE 的访问控制方案缺乏对数据属主访问策略灵活性的支持。因此，有必要研究灵活的支持系统属性撤销及恢复的访问控制方案，且无需 DO 花费较大的计算开销。

3 相关基础

3.1 理论基础

3.1.1 双线性映射

设$\mathbb{G}_1$，$\mathbb{G}_2$都是 q 阶的循环群，其中 q 为素数。如果映射 $e:\mathbb{G}_1\times\mathbb{G}_1\rightarrow\mathbb{G}_2$满足以下 3 条性质：

①双线性(Bilinear)。对任意的 $a,b\in\mathbb{Z}_q^*$，任意的 $P,Q\in\mathbb{G}_1$，$e(aP,bQ)=e(P,Q)^{ab}$。

②非退化性(Non-Degenerate)。映射 e 不是把$\mathbb{G}_1\times\mathbb{G}_1$所有的元都映射到$\mathbb{G}_2$的单位元上。那么，如果 g 是$\mathbb{G}_1$的生成元，则 $e(g,g)$是$\mathbb{G}_2$的生成元。

③可计算性(Computable)。对任意的 $P,Q\in\mathbb{G}_1$，都存在有效的算法计算 $e(P,Q)$。

那么称 e 是一个双线性映射。通常把$\mathbb{G}_1$作为加法群，把$\mathbb{G}_2$作为乘法群。

3.1.2 判定双线性问题

双线性 Diffie-Hellman 问题(Bilinear Diffie-Hellman Problem，BDH 问题)：设 g 是循环群$\mathbb{G}_1$的生成元，($\mathbb{G}_1$，$\mathbb{G}_2$，e)中的 BDH 问题定义为：给定任意四元组(g,g^a,g^b,g^c)，计算 $r=e(g,g)^{abc}\in\mathbb{G}_2$，其中任取的 $a,b,c\in\mathbb{Z}_q^*$。

判定双线性 Diffie-Hellman 问题(Decisional Bilinear Diffie-Hellman Problem，DBDH 问题)：设 g 是循环群$\mathbb{G}_1$的一个生成元，$r\in\mathbb{G}_2$，$a,b,c\in\mathbb{Z}_q^*$且未知，给定一个五元组(g,g^a,g^b,g^c,r)，判定 $r=e(g,g)^{abc}$是否成立。

3.2 AB-ACER 方案

AB-ACER 方案[6]基于 CP-ABE 构造，并且采用了 Shamir[15]的门限秘密共享机制。由于本文方案采用了相同的定义，这里先给出 AB-ACER 方案的相关定义及算法步骤[6]。

定义 1(Key Encrypting Key，KEK) 用于重加密密钥的加密，它是通过 KEK 树[13]分发给用户的，KEK 树是一棵二叉树，由 CSP 管理和存储。

定义 2(用户路径密钥，User Path Key，UPK) 在 KEK 树中，每个叶子节点 v_j 到树根包含一个 KEK 集合，用$\{\exists v_j\in V:KEK_j\}$表示，$V$ 为树中的所有节点。集合$\{\exists v_j\in V:KEK_j\}$称为一个用户的用户路径密钥 UPK[6]。

AB-ACER 方案包括 6 个算法步骤[6]，具体描述如下。

①Setup：系统初始化。生成系统公开参数 PK 和主密钥 MK。

②AttrKeyGen(MK,Λ,U)：私钥产生算法。该算法输出用户私钥集合，其中，$\Lambda\subset A$，集 $U\subset u$。

③KEKGen(U)：密钥加密密钥产生算法。该算法生成密钥 KEK 集合，即为 U 中的每个用户产生一个 KEK 密钥集，KEK 密钥用于加密重加密密钥 K_{λ_y}。

④Encrypt(PK,M,Γ)：加密算法。该算法用于数据属主对明文的加密，输出为关联访问结构的密文 CT。

⑤ReEncrypt(CT,G)：重加密算法。该算法由 CSP 执行对密文的重加密，输出为重加密后生成的重加密密文 CT'。

⑥Decrypt(CT',SK,K_Λ)：解密算法。当且仅当用户属性集 Λ 满足访问结构 T 且用户属性集 Λ 中存在未被撤销的属性时，用户可以解密出原始明文，K_Λ 为用户组属性密钥集。

4 AB-ACVE 方案构造

本节提出基于虚拟扩充属性的访问控制方案 AB-ACVE (Attribute-Based Access Control with Virtual Extension)，其基于 AB-ACER[6]进行构造，核心在于针对访问结构树中代表属性的每个叶子节点建立正、负属性，从而建立一个扩展的访问结构树。在 DO 加密阶段，基于扩展的访问结构树进行加密生成密文，由此将提供一个“全策略”的访问控制机制，当用户属主需要灵活撤销或恢复某个系统属性的访问策略时，可以通过 CSP 完成，而无需 DO 参与，因此可充分利用云计算环境的资源优势，实现灵活的访问策略变更。

4.1 方案体系结构

现有云存储访问控制方案大都引入了可信第三方，本文方案同样也是由云存储服务者、数据属主、可信第三方及普通用户组成，如图 1 所示。其中，云存储服务者具有丰富的计算及存储资源，并向外提供存储访问服务。

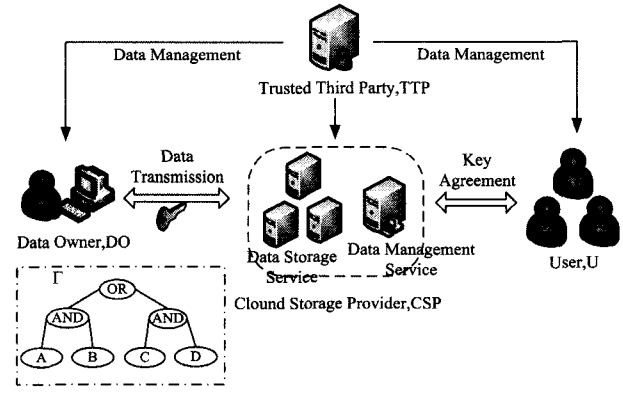

图 1 方案体系结构

①可信第三方(Trusted Third Party，TTP)：主要用于生成系统初始的即公开参数和主密钥，在本文方案中，TTP 作为云存储系统模型中一个完全可信的参与者。

②数据属主(Data Owner，DO)：表示客户端上拥有原始明文数据的用户属主，在方案中，DO 用自己的访问策略加密明文，将密文存储到云存储服务器。

③普通用户(User，U)：用户可以读取云存储服务器上的密文，如果一个用户 $u\in U$，当且仅当他拥有的属性集合满足

密文的访问策略时，能够解密得到明文。

④云存储服务提供者(Cloud Service Provider，CSP)：CSP为用户提供数据存储服务。这里假设CSP不可完全信任，即它将诚实地执行各算法任务，但是也会尽力获取包括访问策略、明文在内的机密信息。

4.2 相关定义

定义3 设$\omega=\{u_1,u_2,\cdots,u_n\}$是用户集全域。其中，$n$是系统中的用户总数。

定义4 设$A=\{\lambda_1,\lambda_2,\cdots,\lambda_q\}$是属性集全域。其中，$q$为群$\mathbb{G}_1$的阶。

定义5 设$G_i\subset\omega$为拥有同一个属性λ_i的用户集，G_i称为一个用户组属性。

定义6 设$\mathcal{G}=\{G_1,G_2,\cdots,G_p\}$为用户组属性的全域。

4.3 算法构造

方案算法中，生成主密钥MK和公开参数PK的算法$Setup$、用户私钥SK生成算法、为用户子集U生成其用户共享密钥集的算法$KEKGen(U)$均保留原有的算法构造。为保证算法的完整性，这里先给出$Setup$及$AttrKeyGen$的算法构造[6]。

(1)$Setup$

$PK=\{g,h=g^{\beta},e(g,g)^{\alpha}\}$

$MK=\{\beta,g^{\alpha}\}$

其中，α,β随机选择且$\alpha,\beta\in\mathbb{Z}_q^*$，$\mathbb{G}_1$是阶为$q$的加法群，$g$是群$\mathbb{G}_1$的一个生成元。$\mathbb{G}_2$是阶为$q$的乘法群，$e$是$\mathbb{G}_1\times\mathbb{G}_1\rightarrow\mathbb{G}_2$的双线性映射。

(2)$AttrKeyGen(MK,\Lambda,U)$

$SK_u=(D=g^{(\alpha+r)/\beta},\forall\lambda_i\in\Lambda:D_i=g^r\cdot H(\lambda_i)^{r_i},D_i'=g^{r_i})$

其中，$r\in\mathbb{Z}_q^*$针对每个用户随机选择，Λ是用户U的属性集，且$\Lambda\subseteq A$，为每个属性$\lambda_i\in\Lambda$随机选择$r_i\in Z_q^*$。

(3)如同参考文献[6]中的构造，采用用户与CSP之间的共享密钥KEK来加密一组不同访问策略子树的密钥密文重加密密钥k_{λ_y}，并将其作为该文件密文对应的一个消息头Hdr，且$Hdr=(\forall y\in Y:\{E_{KEK}(k_{\lambda_y})\})$。

本文方案需要新增或重构的算法具体描述如下。

(4)$Encrypt(PK,M,\Gamma')$：该算法对访问策略树进行属性扩充后，由数据属主DO执行，具体构造如下：

$$CT=(\Gamma',\widetilde{C}=M\cdot e(g,g)^{\alpha s},C=g^{\beta s},\forall y\in Y:C_y^+=g^{q_y^+(0)},C_y'^+=H(\lambda_y^+)^{q_y^+(0)},C_y^-=g^{q_y^-(0)},C_y'^-=H(\lambda_y^-)^{q_y^-(0)})$$

其中，Γ'表示对访问结构树添加叶子节点正负属性节点后扩展的访问树，具体扩充方式为：原有叶子节点变为“AND”内部节点。M代表待加密的明文，$\alpha,\beta,s\in\mathbb{Z}_q^*$，$y^+$代表某个叶子节点的正属性，$y^-$代表某个叶子节点的负属性。这里，$H(\lambda_y^+)$，$H(\lambda_y^-)$是传统CP-ABE算法中定义的公开映射函数，将属性λ_y^+，λ_y^-分别映射为群$\mathbb{G}_2$上的一个随机元素。

(5)$ReEncrypt(CT,G)$：该算法由CSP执行，在原有算法基础上重构。对属性组$G_y\in G$，任意选择一个重加密密钥$k_{\lambda_y}\in\mathbb{Z}_q^*$，完成密文的重加密，具体构造如下：

$$CT'=(\Gamma',\widetilde{C}=M\cdot e(g,g)^{\alpha s},C=g^{\beta s},\forall y\in Y:C_y^+=g^{q_y^+(0)},C_y'^+=(H(\lambda_y^+)^{q_y^+(0)})^{k_{\lambda_y}},C_y^-=g^{q_y^-(0)},C_y'^-=(H(\lambda_y^-)^{q_y^-(0)})^{k_{\lambda_y}})$$

(6)$Decrypt(CT',SK',K_\Lambda)$：该算法由需要访问加密文件的用户$u$执行。用户$u$首先从CSP获取$Hdr$，同文献[6]一样获得重加密密钥$k_{\lambda_y}$并更新其$SK$为$SK'$。

$SK_u'=(D=g^{(\alpha+r)/\beta},\forall\lambda_i\in\Lambda:D_i=g^r\cdot H(\lambda_i)^{r_i},D_i'=(g^{r_i})^{1/K_{\lambda_i}})$

定义递归算法$DecryptNode(CT',SK',x)$，其中x表示所有的叶子节点。

$$DecryptNode(CT',SK',x)=\begin{cases}e(D_i,C_y^+)/e(D_i',C_y'^+)=e(g,g)^{rq_y^+(0)}\\e(D_i,C_y^-)/e(D_i',C_y'^-)=e(g,g)^{rq_y^-(0)}\\\perp\end{cases}$$

得到每个虚拟叶子节点的$e(g,g)^{rq_y^{\pm}(0)}$，利用基于门限的共享秘密算法，最终仍然可以得到$e(g,g)^r$，通过$M=\widetilde{C}/e(C,D)/(e(g,g)^r)$[6]恢复明文。

4.4 访问策略属性撤销与恢复

引入扩充的访问树Γ'后，对于数据属主对系统属性的撤销及恢复，无需DO对明文做重加密的工作，而由计算资源丰富的CSP来完成。

(1)当要撤销某些系统属性时，DO同样利用共享密钥KEK将撤销的属性集T加密并发送给CSP，CSP执行$ReMoveEncrypt(CT',T)$算法。对$\forall y\in T$，CSP针对每个撤销的系统属性λ_y随机选择$s_{\lambda_y}\in\mathbb{Z}_P^*$，对密文进行重加密，该算法构造如下：

$$CT'=(\Gamma',\widetilde{C}=M\cdot e(g,g)^{\alpha s},C=g^{\beta s},\forall y\in Y:C_y^+=g^{q_y^+(0)},C_y'^+=(H(\lambda_y^+)^{q_y^+(0)})^{k_{\lambda_y}},C_y^-=g^{q_y^-(0)},\forall y\in T_i:C_y'^-=(H(\lambda_y^-)^{q_y^-(0)+s_{\lambda_y}})^{k_{\lambda_y}})$$

(2)DO要恢复某些系统属性时，同样利用共享密钥KEK将恢复的属性集T'加密并发送给CSP，CSP执行$ReCoverEncrypt(CT',T')$算法。对$\forall y\in T'$，CSP对密文进行重加密，该算法构造如下：

$$CT'=(\Gamma',\widetilde{C}=M\cdot e(g,g)^{\alpha s},C=g^{\beta s},\forall y\in Y:C_y^+=g^{q_y^+(0)},C_y'^+=(H(\lambda_y^+)^{q_y^+(0)})^{k_{\lambda_y}},C_y^-=g^{q_y^-(0)},\forall y\in T':C_y'^-=(H(\lambda_y^-)^{q_y^-(0)+s_{\lambda_y}})^{k_{\lambda_y}}/(H(\lambda_y^-)^{s_{\lambda_y}})^{k_{\lambda_y}})$$

以上方案的构造使得数据属主的访问策略的变更更加灵活，并且不需要数据属主做重加密工作。

5 安全性与效率分析

5.1 安全性证明

(1)算法安全性分析

AB-ACVE基于AB-ACER方案构造，主要区别在于在加密算法中扩充了访问策略树，为每个叶子节点建立了正负属性节点，加密算法针对扩充的访问策略树，解密算法仍然需要用户属性满足访问策略树；此外，当用户属主修改其访问策略时，构造了CSP的重加密算法。由于本文在密文生成与解密算法的安全性方面[7]已对AB-ACER算法的安全性进行证明，因此AB-ACVE方案的算法安全性就等同于AB-ACER方案算法的安全性。

(2)访问策略的机密性

本文方案的重加密仍然仅仅针对访问结构树的叶子节点。当DO改变访问策略时，通过AB-ACER方案中采用的

KEK 密钥树机制，将需要更新的属性集合加密后发送给 CSP，而 CSP 解密获取变更属性集合后，采用 *ReMoveEncrypt*(CT', T)或 *ReCoverEncrypt*(CT', T')算法重加密密文，在算法构造中也对改变后的属性集对应的叶子节点做了重加密，不会涉及访问策略树的中间节点，因此访问控制策略仍然是安全的。

(3)数据机密性

当 DO 删除属性时，由于重加密算法构造中，CSP 修改了将要删除属性的虚拟节点(负属性节点)的秘密，按照 Shamir 秘密共享方案，分享秘密的合作者减少了，即其门限小于 $\tau-1$，这里 τ 表示分享秘密的合作者门限，即 $e(D_i, C_{y^-})/e(D'_i, C'_{y^-}) \neq e(g,g)^{rq_{y^-}(0)}$，从而无法恢复出 $e(g,g)^{\alpha}$，因此，访问用户将无法解密得到明文，从而保证了数据的机密性。

5.2 效率分析

AB-ACVE 与 AB-ACER 方案在权限撤销及恢复方面的效率分析如表 1 所列。

表 1 策略属性撤销与恢复开销的比较

变更	方案名称	DO 的计算开销	CSP 的计算开销
属性撤销	AB-ACER	$2(n-\lvert T\rvert)\cdot t_e+t_\varepsilon$	$(n-\lvert T\rvert)\cdot t_e$
	AB-ACVE	0	$\lvert T\rvert\cdot t_e$
属性恢复	AB-ACER	$2(n+\lvert T\rvert)\cdot t_e+t_\varepsilon$	$(n+\lvert T\rvert)\cdot t_e$
	AB-ACVE	0	$\lvert T\rvert\cdot t_e$

其中，t_ε 表示一次双线性对运算所需时间，t_e 表示一次模幂运算时间，n 表示访问结构树 Γ' 的属性个数，$|T|$ 表示策略变更属性集中属性的个数，且 $|T|\leqslant n$。

由表 1 可知，当策略属性变更时，AB-ACVE 方案对 DO 计算开销有极大改善，对 CSP 的计算开销也有着较大提升。但这样的计算开销减少是以首次加密明文的计算开销为代价的，如表 2 所列。

表 2 首次生成密文开销的比较

方案名称	DO 的计算开销	CSP 的计算开销
AB-ACER	$2n\cdot t_e+t_\varepsilon$	$n\cdot t_e$
AB-ACVE	$4n\cdot t_e+t_\varepsilon$	$2n\cdot t_e$

由表 2 比较可知，本文的 AB-ACVE 方案在密文首次生成时，DO 及 CSP 在加密阶段都是模幂计算开销，约为 AB-ACER 方案的 2 倍，AB-ACVE 方案在首次加密明文时有更大的计算开销。

由以上分析可知，AB-ACER 方案在权限撤销时相当于要重新做一次明文的重加密工作，而本文 AB-ACVE 方案虽然在首次加密时需要付出更多的计算开销，但换来的是灵活的系统属性的变更支持。通过扩展访问策略树，为每个叶子节点属性建立了相应的虚拟属性，从而使得属性的撤销及恢复仅仅通过 CSP 重加密密文来完成，既保证了密文的保密性，又实现了灵活的策略变更，而无需 DO 花费更多的计算开销。当然，在首次加密明文时，还是需要付出更多的计算开销。

结束语 引入虚拟叶子节点扩充访问控制树的 AB-ACVE 方案，仅在首次加密过程中增加 DO 及 CSP 的计算开销，但可以支持快捷的策略属性撤销及恢复，为访问策略的灵活性提供了一个简便方案。系统属性撤销或恢复时，在无需 DO 参与的情况下，CSP 通过尽量少的重加密密文工作，及时支持系统属性变更，在保证原有 AB-ACER 方案的灵活性、细粒度访问控制的基础上，提升了原有方案系统属性撤销的访问控制的灵活性和高效性。

参 考 文 献

[1] Amazon. com. Amazon s3 Availability Event: July 20, 2008 [OL]. http://status. aws. amazon. com/s3-20080520. html

[2] Arrington M. Gmail Disaster: Reports of Mass Email Deletions [R/OL]. http://www. techcrunch. com/2006/12/28/gmail-disaster-reports-of-massemail-deletions

[3] Krigsman M. Apple's MobileMe Experiences Post-Launch Pain [OL]. http://blogs. zdnet. com/projectfailures/?p=908

[4] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data [C] // CCS. ACM, 2006: 89-98

[5] Su Jin-shu, Cao Dan, Wang xiao-feng, et al. Attribute-Based Encryption Schemes [J] Journal of Software, 2011, 22(6): 1299-1315

[6] 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

[7] Dara K. Microsoft's 2012-11 SkyDrive accidently freezes out Opera users [EB/OL]. [2014-04-20]. http://www. cnet. com/news/microsofts-skydrive-accidently-freezes-out-opera-users

[8] Sahai A, Waters B. Fuzzy Identity-Based Encryption [M] // Advances in Cryptology EUROCRYPT 2005. Springer Berlin Heidelberg, 2005: 457-473

[9] Xiong An-ping, Xu Chun-xiang. Energy Efficient Multiresource Allocation of Virtual Machine Based on PSO in Cloud Data Center [J]. Mathematical Problems in Engineering, 2014, 18(5): 816-830

[10] Bethencourt J, Sahai A, Waters B. Ciphertext-Policy Attribute-Based Encryption [C] // IEEE Symposium on Security and Privacy, 2007(SP'07). IEEE, 2007: 321-334

[11] Pirretti M, Traynor P, McDaniel P, et al. Secure Attribute-Based Systems [J]. Journal of Computer Security, 2010, 18(5): 799-837

[12] Ostrovsky R, Sahai A, Waters B. Attribute-Based Encryption with Non-Monotonic Access Structures [C] // Proceedings of the 14th ACM Conference on Computer and Communications Security. ACM, 2007: 195-203

[13] Yu S, Wang C, Ren K, et al. Attribute Based Data Sharing with Attribute Revocation [C] // Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. ACM, 2010: 261-270

[14] Yu S, Ren K, Lou W. Attribute-based on-demand multicast group setup with membership anonymity [J]. Computer Networks, 2010, 54(3): 377-386

[15] Shamir A. Identity-Based Cryptosystems and Signature schemes [C] // Advances in cryptology. Springer Berlin Heidelberg, 1985: 47-53

[16] Huang Zhi-hong, Wu Li-li, Zhang Bo. Network Security Threats and Prevention on Cloud Computing [J]. Journal of Chongqing University of Technology (Natural Science), 2012, 26(8): 85-90 (in Chinese)
黄志宏，巫莉莉，张波. 基于云计算的网络安全威胁及防范 [J]. 重庆理工大学学报(自然科学)，2012，26(8)：85-90