多权限的属性集加密访问控制方案改进

刘海峰　高月月
（陕西科技大学　陕西 西安 710012）

摘　要　CP-ABE 方案的访问结构是直接外包给云服务器的，这会使得访问策略被公开，而且每个权限都能够在云存储系统中独立地发布属性。由于用户属性的动态性，现在的 CP-ABE 方案并不能直接应用在多权限云存储系统的数据访问控制中。针对这些挑战，提出一种多权限 CP-ABE 访问控制方案。利用隐藏在云存储系统中的策略来保护用户的隐私以及访问策略隐私；采用线性秘密共享方案来实现访问策略。对该方案进行安全性分析，证明其在访问策略的保护和用户权限重新计算的成本方面具有一定的优势。

关键词　属性加密　访问策略　云存储

中图分类号　TP393.08　　**文献标志码**　A　　DOI：10.3969/j.issn.1000-386x.2020.09.052

IMPROVED ENCRYPTION ACCESS CONTROL SCHEME FOR MULTI-PERMISSION ATTRIBUTE SET

Liu Haifeng　Gao Yueyue
(*Shaanxi University of Science and Technology*, *Xi'an 710012*, *Shaanxi*, *China*)

Abstract　The access structure of CP-ABE scheme is outsourced directly to the cloud server, which makes the access policy explode, and each permission can publish attributes independently in the cloud storage system. Due to the dynamic nature of user attributes, the current CP-ABE scheme can not be directly applied to the data access control of multi-permission cloud storage systems. Therefore, in order to meet these challenges, we propose a multi-permission CP-ABE access control scheme. It could protect the privacy and access policy privacy of users by using the policies hidden in the cloud storage system. The linear secret sharing scheme was used to implement the access policy. Finally, the security analysis of the scheme proves that our scheme has some advantages in terms of the protection of access policy and the cost of user rights recalculation.

Keywords　Attribute encryption　Access policy　Cloud storage

0　引　言

云计算自出现以来就受到了广泛的关注，并且发展极为快速，随着云计算的发展逐渐深入，对云计算的安全性方面也提出了更高的要求。为了增强云计算的安全性，密文的检索方案、可验证的数据审计和身份认证等相继提出。云存储是云计算重要的一部分，随着云存储的发展，很多的企业用户都将大量的数据直接外包在云存储服务器中。为了保护数据的安全性，必须采用有效的加密方案来实现云存储中细粒度的访问控制。CP-ABE 在基于密文策略的属性加密中，用户的密钥与属性集有关，密文与访问结构有关。只有用户的属性集满足访问策略的时候，用户才能够解密密文。CP-ABE 能够实现灵活的访问控制，已经被广泛地运用在云存储系统中的访问控制。访问策略是容易泄露的，并且会泄露敏感信息；用户可以具有不同权限的属性，但是数据所有者制定能够访问敏感数据的多个权限。拥有多权限的属性加密用户能够有不同权限下的不同属性，所以更加适合云存储系统的访问控制。因此，本文提出了一种基于多权限属性的加密方案，以实现云存储系统中的细粒度访问控制，从而实现访问

收稿日期：2019－05－13。**刘海峰**，副教授，主研领域：网络信息安全。**高月月**，硕士生。

策略的隐私保护,该方案具有灵活性、实用性和安全性。

1 基础知识

1.1 相关定义

定义 1 双线性映射。设 G 和 G_1 是 $p>2^k$(素数)阶的乘法群,g 为 G 的生成元,那么满足以下三个性质的映射 $e:G\times G\rightarrow G_1$ 为双线性映射。

双线性性:存在 $\forall a,b\in Z_p$, $\forall u,v,u_1,u_2,v_1,v_2,g,h\in G$,那么有 $e(g^a,h^b)=e(g^b,h^a)=e(g,h)^{ab}$,$e(u_1\times u_2,v)=e(u_1,v)e(u_2,v)$,$e(u,v_1\times v_2)=e(u,v_1)e(u,v_2)$。

非退化性:$\exists u,v\in G$,使得 $e(u,v)\neq 1$,其中 1 是 G_1 的单位元。

可计算性:$\forall u,v\in G$,存在一个高效的多项式时间算法计算 $e(u,v)$。

定义 2 访问结构。设 $\Omega=\{L_1,L_2,\cdots,L_n\}$,$|\Omega|=n$ 代表系统所有的属性集,而且每个属性 L_i 的取值集合是 $F_i=\{v_{i1},v_{i2},\cdots,v_{in_i}\}$,其中 n_i 是 F_i 的阶。用户的属性列表为 $w=\{l_1=v_{1t_1},l_2=v_{2t_2},\cdots,l_j=v_{jt_j}\}$,其中 $v_{jt_j}\in F_j$,j 是 w 的阶。使用树型结构构建访问结构 FW,而且 FW 的内部节点代表关系,分别为“与”门和“或”门,而所有的叶子节点代表属性。

定义 3 线性秘密共享方案。如果在参与者集合 P 上的一个秘密共享方案满足以下 2 个条件,那么就称其为 Z_p 上的线性秘密共享方案:

1) 每个实体的秘密份额构成 Z_p 上的一个向量;

2) 对于每个秘密共享方案,存在一个生成矩阵 $\boldsymbol{B}_{(l\times n)}$,对于矩阵 $\boldsymbol{B}$ 中的每一行 $i=1,2,\cdots,l$,映射 $\rho(i):\{1,2,\cdots l\}\rightarrow P$ 把 $\boldsymbol{B}$ 的每一行映射到参与者 $\rho(i)$,考虑向量 $\boldsymbol{v}=(s,r_2,r_3,\cdots,r_n)^{\mathrm{T}}$,$s\in Z_p$ 是共享秘钥,$r_2,r_3,\cdots,r_n$ 随机选择用来隐藏 s,$\boldsymbol{Bv}$ 是 l 个秘密份额形成的向量,其中 $\lambda_i=(\boldsymbol{Bv})_i$ 表示参与者 $\rho(i)$ 所持有的秘密份额。

1.2 单向匿名密钥协议

参与者的匿名性可以由一个单向匿名密钥方案来实现。假设 Alice(ID_a) 和 Bob(ID_b) 是一个密钥生成中心的用户,他们的主密钥都是 s。Alice 想对 Bob 保持匿名性,那么需要进行以下步骤:

1) Alice 计算 $Q_A=H(ID_a)$,$Q_B=H(ID_b)$ 随机选择数 $r_A\in Z_p^*$ 生成假设名 $P_A=Q_A^{r_A}$,并计算会话密钥 $K_{A,B}=e(d_A,Q_B^{r_A})=e(Q_A,Q_B)^{sr_A}$,最后将假设名 P_A 回复给 Bob。

2) Bob 用他的密钥 d_B 计算会话密钥 $K_{A,B}=e(P_A,d_B)=e(Q_A,Q_B)^{sr_A}$,其中 $d_i=H(ID_i)^s\in G_1$ 是用户的私有密钥,$i\in\{A,B\}$,$H:\{0,1\}^*\rightarrow G_1$ 是强抗冲突散列函数。

1.3 问题重述

1.3.1 系统模型

在云环境中一共有四个实体,分别是数据所有者、云存储的服务器、属性权限和数据用户。

1) 数据所有者:在将数据外包到云存储系统之前,数据的所有者根据在密文上强制执行的访问策略对其进行加密,并负责定义访问策略和模糊策略。一旦撤销了一个用户的属性,所有者必须更新包含所有已撤销属性的部分密文组件。

2) 云存储服务器:云存储服务器是属于数据所有者的共享文件,并且为用户提供访问服务。假设云存储服务器是诚实的,那么云存储服务器不仅应该隐藏数据,还应该隐藏密文中的访问策略。

3) 属性权限:属性权限受信任并且独立管理其各自的属性集。同时,为每个合法用户生成密钥,当一个用户被撤销时,权限将为未撤销的用户生成更新的密钥。

4) 数据用户:权限为每个数据用户生成相关的私钥。因此,只有私钥满足访问控制策略的用户才能够获得数据,而且任何合法的用户都可以在云存储服务器中下载任何的密文。

1.3.2 安全性要求

本文对云存储系统中的访问控制方案有如下三个最基本的要求:

1) 数据的安全性:在云存储系统中,只有满足访问策略的授权用户才能够解密密文获得数据,但是被撤销的用户是不能解密密文的。

2) 抗共谋:云存储中的所有属性加密方案都需要抗共谋。抗共谋的意义是不同的用户通过自己的私钥组合来获取不同的密文信息和访问策略。

3) 策略隐私:数据外包在云存储系统中时,所有的云服务器和没有授权的用户无法获得任何有关密文的信息和访问结构。

2 方案设计及其分析

在多权限的属性集加密访问控制中,如果有较多的用户满足同一数据的访问结构,那么会同时获得相同的访问权限。但是用户的需求也正随着云计算的发

展而改变,对权限的要求也变得多种多样,因此对权限的划分应该更加细粒度化。图 1 为本文系统方案模型。

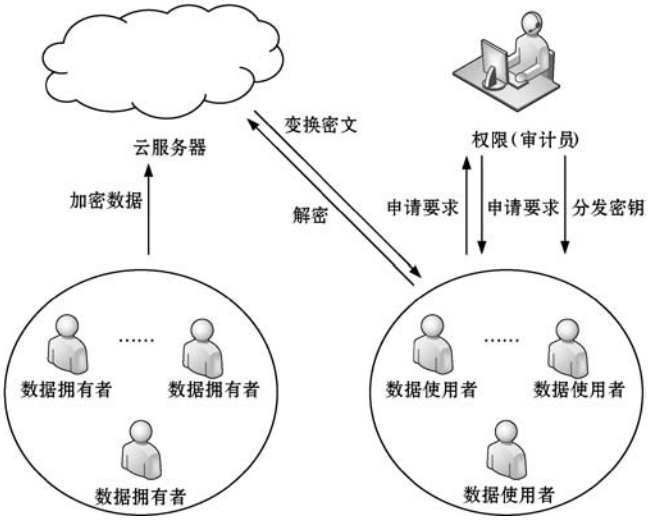


图 1　系统方案模型

2.1　相关定义

本文提出的多权限多属性的访问控制研究主要包括以下四个阶段:

1) Setup:授权中心运行随机算法,为每个属性权限输出相应的公私钥,输出系统的公钥和主密钥。

2) KeyGen:分别运行 Attribute Key Generation(AKG)和 Central Key Generation(CKG)。AKG 是属性权限运行随机算法;CKG 是授权中心运行一个随机算法,然后输入用户的 GID 和主密钥,最后输出用户的私钥。

3) EncSig:数据所有者进行加密和签名。

4) DecVer:用户进行两项工作:解密和验证。

2.2　安全性分析

为了证明本文方案的安全性,采用的是属性集攻击模型,原型是身份安全模型。攻击模型在攻击者 A 和攻击者 C 之间进行,具体步骤如下:

Setup:攻击者 A 提交一组攻击属性列表 $A_C = A_C^1$, $A_C^2, \cdots, A_C^l, l \leqslant K$,每个集合对应一个属性权限。同时提交一个妥协属性权限的列表,其中不包括中心权限。挑战者 C 产生系统参数并且发送给攻击者 A,包括系统公钥,所有诚实属性权限的公钥和妥协属性权限的私钥。

Queries:攻击者 A 能够进行多次的私钥询问,对每一个全局身份,至少存在一个诚实的属性权限 k,攻击者 A 询问的 A_C^k 中的属性少于 d_k;对相同的全局身份,攻击者 A 不能询问同一个属性权限两次。

Challenge:攻击者 A 提交两个等长的消息 M_0 和 M_1。挑战者 C 给出一个随机掷币 $b \in \{0,1\}$,计算在属性集 A_C 作用下的密文 M_b,发送给攻击者 A。

More Queries:攻击者 A 根据上述的限制进行私钥多次询问。

Guess:攻击者输出一个关于 b 的猜测 b'。如果 $b = b'$,则攻击者 A 攻击成功。

2.3　方案分析

本文方案中有 N 个权限 $\{P_1, P_2, \cdots, P_N\}$,且每个权限 P_j 对应一组属性 $L_j, j = 1, 2, \cdots, N$。首先,每个权限 P_j 随机选择一个数 $\beta_j \in Z_p$,对于每一个属性 $x \in L_j$,P_j 选择一个随机数 $v_x \in Z_p$ 用于实现属性撤销。然后,计算公钥为 g^{β_j},其中 β_j 是 P_j 的部分秘密密钥,用户可以使用 g^{β_j} 来混淆属性,β_j 包含在公钥 $PK[j]$ 中。

为了抵抗共谋攻击,当为用户 GID 创建一个秘密密钥时,每个 A_j 使用全局用户身份 GID 来计算 $g^{\alpha_x v_x} H(\mathrm{GID})^{v_x}$。如果两个具有不同 GID 和 GID′的用户试图通过合并他们的密钥来进行共谋攻击,那么在解密的过程中就会出现一些 $e(g,g)^{\mu_i} e(H(\mathrm{GID}), g^{\mu_i})$,从而防止共谋攻击的发生。

为了保护密文的访问策略隐私,数据所有者随机选择一个数字 $a \in Z_p^*$,并在加密消息时计算 $s_y = e((g^{\beta_j})^a, H(\lambda_y))$。通过使用 s_y 来替换访问策略中的属性 λ_y 来实现策略隐私。

关于属性撤销问题,每个权限 P_j 为每个属性 x 分配一个密钥 v_x。一旦出现属性撤销,则与已撤销的属性关联的组件,需要使用 $g^{\alpha_x(v'_x - v_x)}$ 更新密钥和密文中的属性。

2.4　方案构建

设 G_1 和 G_2 是阶为 p 的两个循环群,g 是 G_1 的生成元。$e: G_1 \times G_1 \to G_2$ 是一个双线性映射,还使用一个强抗碰撞散列函数 $H: \{0,1\} \to G_1$,本文基于多权限的属性集加密访问控制方案中隐藏了策略,包括以下五个步骤。

1) 系统初始化。具有一组属性 L_j 的每一个权限 $P_j (j \in N)$ 运行 AASetup 算法,每个属性都没有相交的集合 $(L_i \cap L_j = \varnothing, i \neq j)$。

对于每一个权限 P_j,选择一个 $\beta_j \in Z_p^*$ 和三个随机数 $\alpha_x, y_x, v_x \in Z_p^*$,属性 $x (x \in L_j)$,v_x 是属性的密钥,权限 P_j 的私钥为:

$$SK[j] = (\{\alpha_x, y_x, v_x\}_{x \in L_j}, \beta_j) \tag{1}$$

通过权限计算 $\{e(g,g)^{\alpha_x v_x}, g^{y_x}\}_{x \in L_j}$,公共权限密钥 $A_j (j \in N)$ 是:

$$PK[j] = (\{P_{1,x} = e(g,g)^{\alpha_x v_x}, g^{y_x}\}_{x \in L_j}, g^{\beta_j}) \tag{2}$$

2) 生成密钥。用户在访问数据的时候,请求密钥中心分发密钥,验证用户的身份之后,每个权限运行 KenGen 算法,权限 $A_j (j \in N)$ 给用户属性集 $I_{j,\mathrm{GID}}$ 和相应

的私钥 $K_{j,\mathrm{GID}}$。

$$K_{j,\mathrm{GID}}=(\{D_{1,x}=g^{\alpha_x y_x}H(\mathrm{GID})^{y_x},\ D_{2,x}=H(x)^{\beta_j}\}_{x\in I_{j,\mathrm{GID}}}) \tag{3}$$

$\alpha_x,y_x,v_x,\beta_j\in SK[j]$,用户的私钥是在安全通道中传输的。

3）加密。数据所有者将数据存储在云系统中,然后对数据 MSG 的内容进行加密,定义相关属性的访问策略 T,最后数据所有者使用加密算法对密文再次进行加密。

数据所有者随机选择一个数 $a\in Z_p^*$,计算 $s_y=e((g^{\beta_j})^a,H(\lambda_y))$,其中 $\lambda_y(y\in Y)$ 代表的是一个满足访问策略 T 的属性,Y 是满足访问策略 T 中属性的集合。

为了实现访问策略的隐私保护,数据所有者使用 s_y 来替换访问策略中的属性 λ_y。将访问策略 T 转换为 LSSS 访问矩阵 $\boldsymbol{M}_{m\times h}$,其中 $\boldsymbol{M}_i$ 是 $\boldsymbol{M}$ 的第 i 行。

数据所有者通过下列算法加密数据 MSG。

（1）随机选择一个数 $s\in Z_p^*$ 和一个向量:$\boldsymbol{v}=(s,r_2,r_3,\cdots,r_h)^{\mathrm{T}}\in Z_p^h$。

（2）计算 $\boldsymbol{\mu}_i=\boldsymbol{M}_i\cdot\boldsymbol{v}$。

（3）随机选择一个向量:$\boldsymbol{\omega}=(0,t_2,t_3,\cdots,t_n)^{\mathrm{T}}\in Z_p^h$。

（4）计算 $\boldsymbol{\mu}_i=\boldsymbol{M}_i\cdot\boldsymbol{\omega}$。

（5）在 $\boldsymbol{M}_i$ 中随机选择一个数 $\sigma_i\in Z_p^*$。

（6）计算密文:

$$\begin{aligned}&C_0=MSGe(g,g)^s,h_0=g^a\\&C_{1,i}=e(g,g)^{\mu_i}e(g,g)^{v_{\rho(i)}\alpha_{\rho(i)}},\forall i\in[m]\\&C_{2,i}=g^{\sigma_i},\forall i\in[m]\\&C_{3,i}=g^{y_{\rho(i)}\sigma_i}g^{\mu_i},\forall i\in[m]\end{aligned} \tag{4}$$

（7）密文 CT 外包在云存储系统中。

$$CT=(C_0,\{C_{1,i},C_{2,i},C_{3,i}\}_{\forall i\in[m]},h_0,(\boldsymbol{M},\boldsymbol{\rho})) \tag{5}$$

4）解密。如果用户的属性集满足访问策略,那么就可以获得数据 MSG。首先,用户计算 $s'=e(h_0,H(x)^{\beta_j})=e(g^a,H(x)^{\beta_j})$,$\forall x\in I_{j,u}$,其中 $h_0=g^a$ 来源于密文 CT。其次,使用 s' 来替换属性 x,去构造一个属性集 $I'_{\mathrm{GID}}=\{I'_{j,\mathrm{GID}},j\in[N]\}$。用户获取来自 CT 中的访问策略$(M,\rho)$,并计算集 $R'=\{i:(\rho(i)\cap I'_{\mathrm{GID}})_{i\in[m]}\}$。最后,用户选择常量 $c_i\in Z_p^*$,例如 $\sum_{i\in R'}c_iM_i=(1,0,\cdots,0)$,其中只有第 1 位是 1,其他都是 0。解密的具体过程如下:

（1）对于 $i\in R'$,计算:

$$dec(i)=\frac{C_{1,i}e(H(\mathrm{GID}),C_{3,i})}{e(K_{\rho(i),\mathrm{GID}},C_{2,i})}=e(g,g)^{\mu_i}e(H(\mathrm{GID}),g^{\mu_i}) \tag{6}$$

（2）获得明文。

$$MSG=C_0/\prod_{i\in[m]}dec(i)^{c_i} \tag{7}$$

5）用户撤销。用户 GID′的属性集 $\phi_{j,\mathrm{GID}'}$ 支持撤销权限 P_j,为了防止被撤销属性的用户解密密文,拥有属性集 $\phi_{j,\mathrm{GID}'}$ 的未撤销属性的用户将改变他们存储的数据,用户撤销过程主要有两个阶段:

（1）更新密钥。当用户被撤销的时候,权限 P_j 运行 UKeyGen 算法。首先为每个属性 $x\in\phi_{j,\mathrm{GID}'}$ 随机选择一个版本密钥 $v'_x\in Z_p^*$。然后权限 P_j 计算更新后的密钥 $UK_j=\{g^{\alpha_x(v'_x-v_x)},x\in\phi_{j,\mathrm{GID}'}\}$ 和公钥 $P'_{1,x}=P_{1,x}\cdot e(g,g)^{\alpha_x(v'_x-v_x)}=e(g,g)^{\alpha_x v'_x}$。最后在安全的通道内将 UK_j 发送给未撤销的用户和数据所有者。

（2）未撤销用户的密钥更新。当用户收到更新后的密钥 UK_j,运行 SKU 算法更新私钥。

$$\begin{aligned}K'_{j,u}=(&\forall x\in\phi_{j,\mathrm{GID}'}:D'_{1,x}=D_{1,x}\cdot UK_j=g^{\alpha_x y'_x}H(\mathrm{GID})^{y_x}\\&D'_{2,x}=D_{2,x}\\&\forall x\in\phi_{j,\mathrm{GID}'}:D'_{1,x}=D_{1,x},D'_{2,x}=D_{2,x})\end{aligned} \tag{8}$$

密钥 UK_j 与已撤销的用户 GID′相关联,因此,非撤销的用户与撤销的用户能够区分,被撤销的用户无法接受更新之后的密钥 UK_j。

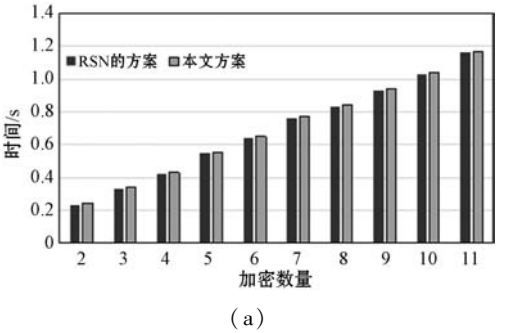
2.5 方案对比

本文方案与其他学者研究之间的对比如表 1 所示。

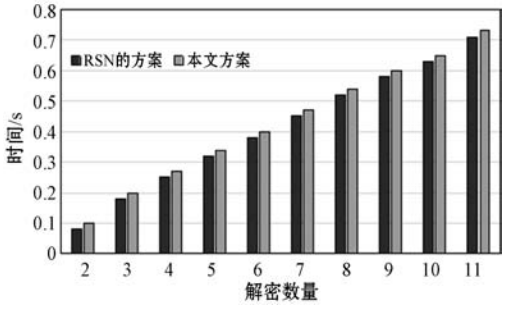
表 1 方案比对

方案对比	公钥	隐藏策略	用户撤销	权限
文献[1]	树结构	有	无	单权限
文献[2]	树结构	有	无	单权限
文献[3]	LSSS	无	有	多权限
文献[4]	LSSS	无	无	多权限
文献[5]	LSSS	无	有	多权限
本文方案	LSSS	有	有	多权限

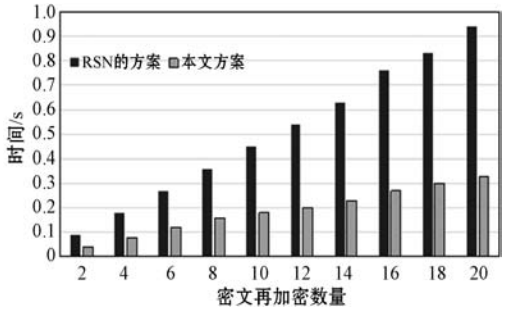
将本文方案与 RSN 方案的加密解密和再加密的计算过程进行仿真,图 2 为本文在 Windows 7 系统 CoreTM i5-4647 在 4 GB 内存中实现加密、解密和密文再加密的时间对比。



(a)



(b)



(c)

图 2　方案对比结果

假设从授权中心获得 10 个属性,在每次实验中取得的结果是 20 次的平均值,结果对比如图 2 所示。可以看出,本文方案在加密解密时间上和 RSN 的方案相差不多,但是本文在密文再加密的时间上却远远比 RSN 方案少,因此总体上具有一定的优势,计算效率也更高。

3　结　语

本文研究了云存储系统中多权限的属性集加密访问控制方案的改进,提出了一个安全的分散属性加密方案,用于设计一个具有策略隐私的访问控制方案。本文的访问控制方案还支持数据的隐私保护,采用的是更加灵活的线性秘密共享方案,同时还支持对多权限的属性加密方案的用户撤销,从而降低了用户撤销的时间成本和计算成本。最后通过实验验证了本文方案的可行性。

参 考 文 献

[1] Phuong T V X, Yang G, Susilo W. Hidden ciphertext policy attribute-based encryption under standard assumptions[J]. IEEE Transactions on Information Forensics and Security, 2016,11(1):35 - 45.

[2] Xu R H, Lang B. A CP-ABE scheme with hidden policy and its application in cloud computing[J]. International Journal of Cloud Computing, 2015,4(4):279 - 298.

[3] Yang K, Jia X. DAC-MACS: Effective data access control for multi-authority cloud storage systems[M]//Security for Cloud Storage Systems. Springer, 2014:59 - 83.

[4] Lewko A, Waters B. Decentralizing attribute-based encryption[M]//Advances in cryptology-EUROCRYPT 2011. Springer, 2011:568 - 588.

[5] Ruj S, Stojmenovic M, Nayak A. Decentralized access control with anonymous authentication of data stored in clouds[J]. IEEE Transactions on Parallel and Distributed Systems,2014, 25(2):384 - 394.

[6] 赵志远,王建华,徐开勇,等. 面向云存储的支持完全外包属性基加密方案[J]. 计算机研究与发展,2019,56(2):442 - 452.

[7] 张兴兰,崔遥. 基于群签名的属性加密方案[J]. 网络与信息安全学报,2019,5(1):15 - 21.

[8] 林素青. 支持访问更新的可验证外包属性加密方案[J]. 网络与信息安全学报,2019,5(1):37 - 49.

[9] 谭呈祥. 浅谈云计算环境下一种新的属性加密匿名算法研究[J]. 电脑知识与技术,2019,15(5):46 - 47.

[10] 朱淑文,钟伯成,丁佳蓉,等. 医疗传感网中基于属性加密的访问控制研究[J]. 单片机与嵌入式系统应用,2019,19(2):23 - 26.

[11] 高峰,谭晶晶. 云环境下基于属性多层次加密算法研究[J]. 科技通报,2018,34(12):124 - 128.

[12] 郝泽晋,梁志鸿,张游杰,等. 大数据安全技术概述[J]. 内蒙古科技与经济,2018(24):75 - 78.

[13] 荣静,殷新春. 可追踪并撤销属性的密文策略属性基加密方案[J]. 北京工业大学学报,2019,45(2):143 - 152.

[14] 曾萍,钱进,穆成新,等. 一种轻量级的雾计算属性基外包加密算法[J/OL]. 计算机应用研究:1 - 5[2019 - 05 - 13]. https://doi.org/10.19734/j.issn.1001 - 3695.2018.06.0556.

[15] 王旭东. 基于密文搜索的 LBS 位置隐私保护机制研究[D]. 兰州:兰州理工大学,2018.

[16] 周玉坤. 云存储系统中数据去重安全性方法研究[D]. 武汉:华中科技大学,2018.

[17] 谭跃生,鲁黎明,王静宇. 基于同态加密的密文策略属性加密方案[J/OL]. 计算机工程与应用:1 - 8[2019 - 05 - 13]. http://kns.cnki.net/kcms/detail/11.2127.TP.20181129.0845.002.html.

[18] 齐芳,李艳梅,汤哲. 可撤销和可追踪的密钥策略属性基加密方案[J]. 通信学报,2018,39(11):63 - 69.

[19] 张恩,裴瑶瑶,杜蛟. 基于 RLWE 的密文策略属性代理重加密[J]. 通信学报,2018,39(11):129 - 137.

[20] 马华,党乾龙,王剑锋,等. 基于属性加密的高效密文去重和审计方案[J]. 电子与信息学报,2019,41(2):355 - 361.