一种灵活的多权威属性协同访问控制方案

彭宗凤[1]，彭长根[1,2]，丁红发[1,3]
〔1.贵州大学公共大数据国家重点实验室（计算机科学与技术学院），贵州贵阳 550025；2.贵州大学密码学与数据安全研究所，贵州贵阳 550025；3.贵州财经大学信息学院，贵州贵阳 550025〕

摘 要：属性协同访问控制是一种能解决多人协同访问的新型访问控制方案，但已有属性协同访问控制方案中的单个属性权威使其存在单点瓶颈问题，且协同功能缺乏灵活性。针对该问题，提出了一种更灵活的多权威属性协同访问控制方案。所提方案给出了协同访问结构的形式化定义，并引入多属性权威的概念，由多个属性权威负责管理属性和分发属性所对应的用户私钥，减轻了单个属性权威的计算负载。在实现协同时，利用密钥协商的思想，使得参与协同的任意两个属性权威仅需一次通信即可得到协同密钥。方案不需为参与协同的用户建立用户组，进一步使得协同更具灵活性、更贴合实际。安全性分析表明，所提方案能保证数据机密性、抵抗共谋攻击，与已有属性协同访问控制方案相比，具有更小的协同通信代价。

关键词：属性协同；访问控制；单点瓶颈；多属性权威
中图分类号： TP309 **文献标识码：** A

An attribute-based flexible collaborative access control scheme with multi-authority

Peng Zongfeng[1], Peng Changgen[1,2], Ding Hongfa[1,3]
〔*1. State Key Laboratory of Public Big Data (College of Computer Science and Technology), Guizhou University, GuizhouGuiyang 550025;2. Institute of Cryptography and Data Security, Guizhou University, GuizhouGuiyang 550025;3. College of Information, Guizhou University of Finance and Economics, GuizhouGuiyang 550025*〕

Abstract: Attribute-based collaborative access control is a new type of scheme, where multiple users having different attribute sets can collaborate to gain access permission, while, there existing single-point bottleneck and lack of more flexible collaboration. To this end, an attribute-based more flexible collaborative access control scheme with multi-authority was proposed. Firstly, given the formalized definition of collaboration access control, and introduced the notion of multiple attribute authorities, that responsible for managing all attributes and distributing corresponding secret keys for users, which reduces the computation overhead of single attribute authority. And then, only need one-time communication between arbitrary two attribute authori-ties to get collaboration key, to achieve collaboration, by using the idea of key exchange without user group, and further make the collaboration more flexible and practical. Security analysis show that the proposed scheme can provide data confi-dentiality and resist collusion attack, and have more flexible collaboration and less communication overhead of collaboration compared with existing scheme.

Key words: attribute-based collaboration; access control; single-point bottleneck; multi-authority

1 引言

近年来，数据呈爆炸性增长，使得云存储服务迅速普及。但数据外包存储至云服务平台时，数据拥有者失去对外包数据的控制权，因此，针对外包数据的访问控制成为保证数据安全性的关键。在云存储环境下，已有学者提出基于密码学的访问控制方案[1~3]，其中基于密文策略的访问控制方案[2]（Ciphertext-Policy Attribute-Based Encryption，CP-ABE）解决了灵活且细粒度的访问控制问题，迅速成为访问控制领域的研究热点。与此同时，云存储环境下多人协同访问需求逐渐增大[4]，访问设备也越来越多，但CP-ABE方案只允许属性集合满足访问结构的单个用户才能解密，无法解决多人协同访问场景下的访问控制问题。

针对该问题，同时考虑到用户来源于多个不同组织或组织内不同部门的特定协同需求，本文基于Xue等人[5]的协同访问控制方案构造了一个更灵活的多权威属性协同访问控制方案，本方案采取单权威与多权威相结合的框架，引入密钥协商的思想，使本方案可以在不需要用户组的情况下实现协同，打破了已有协同方案[5]的局限性，同时避免为来自不同组织的用户协同建立用户组，有效提升了协同效率。此外，本方案中的单权威（即中心权威）不需管理属性和为用户分发私钥，即使中心权威被恶意敌手攻击，敌手也无法恢复出有效的私钥，进一步保证了数据的安全性。具体而言，本文的主要贡献为两方面。

（1）构建更灵活的属性协同访问控制方案。本方案遵循属性的多来源特性，引入多权威的概念，设计一种用户来自不同组织的协同访问控制方案。

（2）提升协同的性能、保证协同的安全性。本方案中任意两个需要参与协同的属性权威只需进行一次通信即可实现合法性认证与协同密钥协商，有效地降低了协同通信开销；同时，由多个属性权威负责管理属性以及密钥的分发，明显地减轻了单个中心权威的计算负载。此外，利用随机化的方法，使得不同用户间无法共谋。

2 相关工作

2005年，Sahai和Waters[1]首次提出了基于属性的加密技术（Attribute-Based Encryption，ABE），该方案首次将身份与属性相关联。2007年，Bethencourt等人[2]构造出CP-ABE方案，该方案利用更为灵活的树形访问结构提供访问控制，但只在通用群模型下证明其安全性。近年来，在CP-ABE方案的安全性[6,7]、效率[8,9]、特定应用领域[4]等得到深入研究。

针对特定的协同领域，协同访问控制方案中的数据安全和隐私依赖多个参与者的协同防护[10]，Willy等人[11]利用合法用户扩展访问策略以实现协同访问，但需要其他加密方法来保证扩展前后的数据完整性。与之相反，有学者从改进和扩展原始ABE或CP-ABE的角度实现协同[12,5]。Li等人[12]提出面向组（Group）的属性加密方案，该方案允许同一组中多个用户合并后的属性集合满足协同访问策略，但其无法灵活控制协同能力。Xue等人[5]基于用户组[12]和转移节点[13]的思想，提出一种可控的属性协同访问控制方案，即在访问策略中规定只有拥有协同属性的用户才能参与协同。

通常，根据CP-ABE的各类衍生方案中参与密钥分配的权威（Authority）数量，可将其分为单权威（Single-Authority）[5,10~12]和多权威（Multi-Authority）[14]两类。在单权威方案[5,10~12]中，只有一个权威中心负责管理全部属性，并且为所有用户生成和分发属性私钥，在单权威方案中，单点（Single-Point）性能瓶颈问题较为突出[15]。因而，为解决用户属性来源于多个权威的问题。Chase等人[16]基于ABE方案首次提出多权威方案，该方案中多个相互独立的权威负责管理属性以及分发相应的私钥，其中包含一个中心权威（Central Authority，CA）。随后，一些没有CA的多权威ABE方案被提出[17]。同样，也有基于CP-ABE的多权威方案研究[18,19]，Ruj等人[20]将Lewko等人[19]的思想应用到访问控制中。

由上述分析可知，已有属性协同访问控制方案[5]仍属于单权威方案，依旧面临单点瓶颈问题以及更复杂的多人协同访问需求。如何使属性

协同访问控制从单权威扩展到多权威，仍无有效解决方案。目前，亟需更加灵活的多权威属性协同访问控制方案，满足跨域大规模用户访问控制的属性管理和私钥分发需求。

3 预备知识

本文所用到的缩略词如表1所示。

表1 相关名词及缩略词

缩略词	含义
CA	Central Authority
AA	Attribute Authority
DO	Data Owner
DU	Data User
CSP	Cloud Service Provider
SK	Secret Key
PK	Public Key
CK	Collaboration Key

本方案的中心权威CA和属性权威AA是可信的，但云服务提供商CSP是“诚实且好奇的”（Honest but Curious）。

3.1 相关定义

定义1：访问结构[21]。设$P=\{P_1,P_2,...,P_n\}$为n个参与者集合，$\mathrm{A}\subseteq 2^P\setminus\{\varnothing\}$是参与者集合的一个非空子集且集合A是单调的，即$\forall B,C$，若$B\in\mathrm{A}$，且$B\subseteq C$，则$C\in\mathrm{A}$。属于A中的集合称为授权集合，否则，称为非授权集合。

定义2：双线性映射。设置两个阶为素数q的乘法循环群G和G_T，g是G的一个生成元。存在一个双线性映射$e:G\times G\to G_T$，满足以下三个性质。

（1）双线性。$\forall g_1,g_2\in G,\forall a,b\in {}_R\mathrm{Z}_p$，都有$e(g_1^a,g_2^b)=e(g_1,g_2)^{ab}$。

（2）非退化性。$\exists g_1,g_2\in G$，有$e(g_1,g_2)\neq 1$。

（3）可计算性。$\forall g_1,g_2\in G$，计算$e(g_1,g_2)$是有效函数。

3.2 困难假设

定义3：判定双线性Diffie-Hellman（Decisional Bilinear Diffie-Hellman，DBDH）问题。假设给定两个阶为q的循环加法群G和循环乘法群G_T、一个双线性映射$e:G\times G\to G_T$，G的生成元为g。DBDH问题就是给定一个四元组(g,g^a,g^b,g^c)，$a,b,c,z\in\mathrm{Z}_p$，判断这个四元组是DBDH四元组$(g,g^a,g^b,e(g,g)^{abc})$，还是随机四元组(g,g^a,g^b,g^z)。如果在多项式时间内解决DBDH的概率是可忽略的，那么DBDH问题是困难的。

4 模型定义

4.1 MA-ABCAC方案模型

图1给出本文所提MA-ABCAC（Attribute-based Collaborative Access Control with Multi-Authority）方案模型。

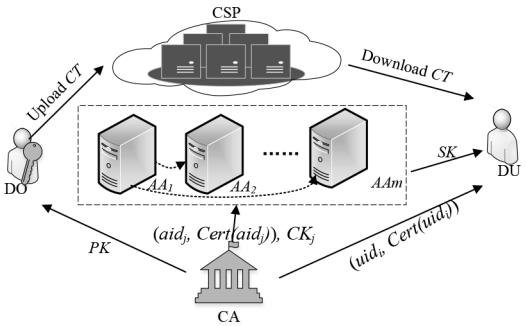

图1 MA -ABCAC方案模型

为防止不同权威间的用户共谋，CA分别为请求注册的AA和用户生成标识符$aid_j,j\in(1,m)$和$uid_i,i\in(1,n)$。AA负责管理用户属性及为用户分发私钥，AA验证用户合法性后将私钥SK_{aid_j,uid_i}发送给用户，简便起见，将SK_{aid_j,uid_i}记作$SK_{j,i}$。协同过程中，参与协同的任意两个AA间只需进行一次通信即可得到协同所需的通信密钥，即协同密钥。

4.2 安全模型

本方案算法的安全性基于可选择安全，其形式化定义如下。

（1）初始化：敌手$\mathcal{A}$向挑战者$\mathcal{C}$公开其要挑战的访问结构$\mathbb{A}^*$。

（2）系统建立：挑战者运行密钥生成算法，生成公钥和私钥，并将公钥发送给敌手。

（3）询问阶段1：敌手询问关于属性集合钥S_i

的私钥，但必须满足$S_i \notin \mathbb{A}^*$。

（4）挑战：敌手向挑战者发送消息m_0, m_1，挑战者随机投掷一枚硬币$b \in \{0,1\}$，在$\mathbb{A}^*$下对m_b进行加密，并将结果返回给敌手$\mathcal{A}$。

（5）询问阶段2：重复询问阶段1的步骤。

（6）猜测：敌手$\mathcal{A}$输出对b的猜测b'，若$b'=b$，则敌手赢得游戏。

定义4：IND-CPA安全。若多项式时间敌手拥有可忽略的优势攻破上述游戏，则所提MA-ABCAC方案是IND-CPA安全的，敌手优势为$\left|\Pr[b'=b]-1/2\right|$。

5 MA-ABCAC方案

在协同密钥生成过程，结合Diffie-Hellman密钥协商[22]的思想，使协同过程中的任意两个AA只需一次通信即可得到协同密钥，协同密钥能聚集不同用户的解密权限，是实现协同访问的关键。协同密钥生成过程如图2所示，简单起见，仅描述两个AA间的通信过程，协同访问策略为$\{\{t_1,t_2\},\{t_3\}\}$，在协同场景下一个用户无法同时拥有属性集合$\{t_1,t_2,t_3\}$，如妇产科医生不可能拥有精神科医生的属性。其中，t_3表示协同属性，即允许其他拥有属性t_3的用户参与协同，此类用户称作协同者。

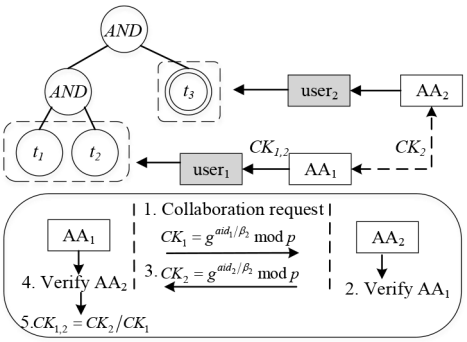

图2 协同密钥生成示意图

5.1 协同访问结构

在协同场景下，由数据拥有者指定访问结构以及允许参与协同的属性，因此解密密钥中的属性集合由不同用户的属性集合构成，若属性集合全部来自同一个参与者（用户），则访问结构“退化”为定义1中的一般访问结构。本方案在定义1的基础上，给出协同访问结构的定义。

定义5：设参与者集合为$\psi=\{\psi_1,\psi_2,...,\psi_n\}$，其中，$\psi_i=\{a_{i,1},a_{i,2},...,a_{i,n_i}\}$，故协同场景下的参与者集合为$\psi=\{\{a_{1,1},a_{1,2},...,a_{1,n_1}\},...,\{a_{n,1},a_{n,2},...,a_{n,n_n}\}\}$，$\mathbb{A}\subseteq 2^{\psi}\setminus\{\varnothing\}$是参与者集合的一个非空子集，对$\forall B,C$若$B\in\mathbb{A}$，且$B\subseteq C$，则$C\in\mathbb{A}$，即$\mathbb{A}$满足单调性。属于$\mathbb{A}$中的集合称为授权集合，否则，称为非授权集合。本方案中参与者集合指的是参与者的属性集合。

5.2 算法构造

本方案根据上述协同访问结构的定义进行算法构造。

算法1：初始化算法

$\mathbb{G},\mathbb{G}_T$是两个阶为素数q的乘法循环群，g是群$\mathbb{G}$的生成元，定义双线性映射$e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$，Hash函数$H:\{0,1\}^*\to\mathbb{G}$。

$CASetup(\lambda)$：定义用户集合U，属性权威集合I。输入安全参数λ，选择$a\in_R\mathbb{Z}_p$作为CA的密钥，生成签名密钥和验证密钥对(sk_{CA}, vk_{CA})，vk_{CA}是公开的。当合法的AA提出注册请求时，CA生成AA的标识符为$aid\in_R\mathbb{Z}_p$，证书为$Cert(aid)$。当合法用户提出注册请求时，CA为用户生成标识符$uid\in_R\mathbb{Z}_p$，选择$\Lambda_{uid}\in_R\mathbb{Z}_p$生成证书$Cert(uid)$，证书中包含$En_{sk_{CA}}(uid,\Lambda_{uid})$。

$AASetup$：定义由属性权威AA_j管理的属性集合为S_{I_j}，选择$\alpha_j,\beta_1,\beta_2\in_R\mathbb{Z}_p$，输出系统公钥为$PK=\{g,e(g,g)^{\alpha_j},H,h_1=g^{\beta_1},h_2=g^{\beta_2}\}$，主密钥为$MSK=\{g^{\alpha_j},\beta_1,\beta_2\}$。

算法2：密钥生成算法

$SKGen$：定义用户uid_i的属性集合$S_i=\{a_{i,1},a_{i,2},...,a_{i,n_i}\}$，$a_{i,k}$表示$S_i$中第k个属性，$n_i$表示$S_i$中属性总数。AA为属性$a_{i,k}$选择$t_{i,k}\in_R\mathbb{Z}_p$，$1\le k\le n_i$。AA生成用户私钥：

$$SK_{j,i}=\{D_i=g^{\frac{\alpha_j+aid_j}{\beta_1}},\forall k\in[1,n_i]:D_{i,k}=g^{uid_i}H(a_{i,k})^{at_{i,k}},$$

$$D'_{i,k}=g^{t_{i,k}},E_i=g^{\frac{aid_j+uid_i}{\beta_2}}\}。$$

$CKGen$：当两个用户之间需要协同时，如图2中user$_1$需要user$_2$参与协同访问。首先，AA$_1$向AA$_2$发送签名后的协同请求和$CK_1=g^{aid_1/\beta_2}\bmod p$；AA$_2$利用$vk_{CA}$对AA$_1$的合法性进行验证，若AA$_1$是

合法的，则AA_2计算并发送$CK_2 = g^{aid_2/\beta_2} \bmod p$给AA1，反之中止协同密钥生成过程，返回错误输出符$\perp$；最后，若AA_1成功验证CK_2是由AA_2发来的密钥结果，计算协同密钥为$CK_{1,2} = CK_2/CK_1 = g^{aid_2/\beta_2} / g^{aid_1/\beta_2} \bmod p = g^{aid_2 - aid_1/\beta_2} \bmod p$。

算法3：加密算法

Encrypt：数据拥有者首先用对称加密算法加密数据，然后在访问结构$\mathbb{A}$下加密对称密钥κ。选择一个随机数$s \in_R Z_p$，然后计算密文：

$$CT = \{\mathbb{A}, \tilde{C} = \kappa \cdot (\prod_{j \in I_A} e(g,g)^{\alpha_j})^s, C = h_1^s, \bar{C} = h_2^s,$$
$$\forall y \in Y : C_y = g^{q_{y,j}(0)}, C'_y = H(att(y))^{aq_{y,j}(0)},$$
$$\forall x \in X : \hat{C}_x = h_2^{q_{x,j}(0)}\}。$$

算法4：解密算法

Decrypt$(CT, SK, [CK_i])$：首先定义递归算法*DecryptNode*$(CT, S_i, x, uid_i, [CK_i])$，记$x = att(x)$。

①若x是叶子节点，即$x \in Y$，则：

$$DecryptNode(CT, S_i, x, uid_i) =$$
$$\begin{cases} \dfrac{e(D_{i,j}, C_x)}{e(D'_{i,j}, C'_x)} = \dfrac{e(g^{uid_i} H(a_{i,j})^{at_{i,k}}, g^{q_{x,j}(0)})}{e(g^{t_{i,k}}, H(a_{i,j})^{aq_{x,j}(0)})} = e(g,g)^{uid_i q_{x,j}(0)}, x \in S, \\ \perp, x \notin S \end{cases}$$

②若x是非叶子节点，即$x \notin Y$，用z表示节点x的k_x个孩子节点，并将结果存储到集合B_x中。若z不是协同属性，则节点z与uid_i相关联，算法调用*DecryptNode*(CT, S_i, x, uid_i)，并将计算结果存储到变量F_z；若z表示协同属性，则z与用户$uid_{i'}$相关联，$i' \neq i$，调用*DecryptNode*$(CT, S_i, x, uid_{i'}, CK_{i,i'})$，并将计算结果存储到$F'_z$。这意味着除数据请求者之外的其他用户$uid_{i'}$（协同者）能够协同解密节点z，然后计算：

$$F_z = e(\hat{C}_z, E_{aid_i} / E_{aid_{i'}} \bullet CK_{i,i'}) \bullet F_{z'}$$
$$= e(g^{\beta_2 q_{z,j}(0)}, g^{\frac{aid_i + uid_i - (aid_{i'} + uid_{i'})}{\beta_2}} \bullet g^{\frac{aid_{i'} - aid_i}{\beta_2}}) \cdot e(g,g)^{uid_i q_{z,j}(0)},$$
$$= e(g,g)^{uid_i q_{z,j}(0)}。$$

进而协同者将其输出结果F'_z转移到F_z，然后，使用Lagrange多项式插值方法计算F_x，具体为：

$$F_{x,j} = \prod_{z \in B_x} F_z^{\Lambda_{m, B_z^{(0)}}(0)}, where^{m = index(z)}_{B_z' = \{index(z) : z \in B_x\}}$$
$$= \prod_{z \in B_x} (e(g,g)^{uid_i q_{z,j}(0)})^{\Lambda_{m, B_z^{(0)}}(0)}$$
$$= \prod_{z \in B_x} (e(g,g)^{uid_i q_{parent(z)}(index(z))})^{\Lambda_{m, B_z^{(0)}}(0)}$$
$$= \prod_{z \in B_x} (e(g,g)^{uid_i q_{x,j}(m)})^{\Lambda_{m, B_z^{(0)}}(0)} = e(g,g)^{uid_i q_{x,j}(0)} 。$$

其中，拉格朗日系数为$\prod_{b \in B_z, b \neq m} x - b/m - b$，$F_r = DecryptNode(CT, S_i, r, uid_i) = e(g,g)^{uid_i q_{r,j}(0)} = e(g, g)^{uid_i s}$，$F = E(\bar{C}, E_i)/F_r = e(g^{\beta_2 q_{r,j}(0)}, g^{aid_i + uid_i/\beta_2})/e(g, g)^{uid_i q_{r,j}(0)} = e(g,g)^{aid_j \cdot s}$。然后计算对称密钥$\kappa = \tilde{C} \cdot F / e(C, D_i) = \kappa \cdot e(g,g)^{\alpha_j \cdot s} \cdot e(g,g)^{aid_j \cdot s} / e(g^{s \cdot \beta_1}, g^{aid_j + \alpha_j/\beta_1})$。当用户获得对称密钥$\kappa$后，可解密出明文消息M。

6 方案分析

6.1 安全性分析

定理1：若DBDH问题是困难的，则不存在PPT的敌手能以不可忽略的优势赢得第4.2节定义的安全游戏，即所构造的MA-ABCAC方案具有不可区分选择明文攻击（Indistinguishable Chosen-Plaintext Attack, IND-CPA）安全。

证明：若敌手$\mathcal{A}$能以不可忽略的优势ε在IND-CPA安全模型下选择性地攻破本方案，那就存在一个挑战者$\mathcal{C}$能在多项式时间内以不可忽略的优势解决DBDH问题。

（1）初始化：敌手公开要挑战的访问结构$\mathbb{A}^*$。

（2）参数设置：挑战者随机选择$t, \alpha \in_R Z_p$，并设置参数$\beta_1 = \beta, \beta_2 = t\beta, \alpha = ab + c$，$Z = e(g,g)^{\alpha} = e(g,g)^{ab} e(g,g)^{c}$，随机选择$s_i \in Z_P, i \in I$，则有$H = g^{s_i}$，$h_1 = g^{\beta}$，$h_2 = g^{t\beta}$，并将公钥发送给敌手$PK = \{H, h_1 = g^{\beta}, h_2 = g^{t\beta}, Z\}$。

（3）训练阶段1：敌手向挑战者询问属性集合S_i的私钥，$1 \leq i \leq q_1$，$\{a_{i,j}\}$是S_i中的属性，其中j表示S_i中的第j个属性，挑战者选择$t_i, t_{i,j} \in_R Z_p$，$r \in Z_p$，设置$r = aid_j, r_i = uid_i, r'_{i,j} = at_{i,k}$，计算$D_i = g^{ab + c + r/\beta}$，$r^* = t_i - r_i, r'' = t_{i,j} - r'_{i,j}$，则$r + r^* = r - r_i + t_i$，计算$E_i^* = (g^{(r - r_i)/\beta})^{t^{-1}} \cdot g^{t_i/t\beta} = g^{r^* + r/t\beta}$。

挑战者计算$SK_i^* = (D = g^{ab + c + r/\beta}, \forall a_{i,j} \in S_i : D_{i,j} = g^{r^*} H(a_{i,j})^{r''}, D'_{i,j} = g^{r''}, E_i^* = g^{r^* + r/t\beta})$。

（4）挑战：阶段1结束后，敌手将其所要挑战的访问结构$\mathbb{A}^*$和两个明文消息$m_0, m_1 \in G$发送给挑战者。挑战者随机投掷硬币b，随机选择$s \in_R Z_p$，将产生的密文CT^*返回给敌手。注意：敌手询问的属性集合不满足访问结构$\mathbb{A}^*$。

$$CT^{*}=\{\mathbb{A}^{*},\tilde{C}=m_b Z^{s},C=h_1^{s},\bar{C}=h_2^{s},$$
$$\forall y\in Y:C_y=g^{q_y(0)},C_y'=H(att(y))^{aq_y(0)},$$
$$\forall x\in X:\hat{C}_x=h_2^{q_x(0)}\}。$$

（5）训练阶段2：与训练阶段1操作相同，但同样满足$S_i\notin\mathbb{A}^{*}$。

（6）猜测：敌手输出猜测结果$b'\in\{0,1\}$，若$b'=b$，挑战者输出$u'=0$时，表示(A,B,C,Z)是一个有效的DBDH四元组，否则，(A,B,C,Z)是一个随机四元组。所以，当$u=1$时，敌手并没有得到任何有用信息，此时$\Pr[b'\neq b|u=1]=1/2$。当$b\neq b'$时，挑战者随机猜测$u'=1$，有$\Pr[b'=b]=1/2$。当$u=0$时，敌手的优势定义为ADV_{CPA}，故$\Pr[b=b'|u=0]=1/2+ADV_{CPA}$。当$b=b'$，挑战者猜测$u'=0$时，$Pr[u'=u|u=0]=1/2+ADV_{CPA}$。综上，在解决DBDH问题的游戏中挑战者总的优势为

$$\frac{1}{2}Pr[u'=u|u=0]+\frac{1}{2}Pr[u'=u|u=1]-\frac{1}{2}=$$
$$\frac{1}{2}(\frac{1}{2}+ADV_{CPA})+\frac{1}{2}\bullet\frac{1}{2}-\frac{1}{2}=\frac{1}{2}ADV_{CPA}。$$

综上可知，敌手攻击本文方案的优势ADV_{CPA}是可忽略的。因此，本方案是IND-CPA安全的。

证毕。

定理2：MA-ABCAC方案能够抵抗共谋攻击。

证明：所提MA-ABCAC方案中用全局唯一标识符标记用户和AAs，每个用户具备唯一的，因而用户间无法产生共谋。此外，AAs具有唯一的aid，即使不同的AAs管理相同的属性，其管理的属性之间依旧具有可区分性。

尤其针对协同属性，本方案只有在AAs间通过合法性认证后才能进行协同密钥协商，即建立了可信的交互基础，同时只有具备E_i'的用户才具备协同能力，故本方案的协同功能具有抗共谋特性。

6.2 性能分析

本方案建立在Xue等人[5]提出的协同方案之上，故与该方案进行分析与对比，存储通信开销和计算开销对比如表2和表3所示。本节用n_c表示密文中属性总数，n_u表示用户拥有的属性总数，$n_{a,u}$表示用户u中由属性权威a管理的属性总数，$|co|$表示协同属性总数，N_A表示属性权威总数，m表示用户组总数，$|nl|$表示解密时访问树中非叶子节点总数，T_e表示指数操作所需时间，T_p表示双线性配对操作所需时间。

表2 存储和通信开销对比

项目	Xue[5]	本文方案
密文长度	$(2n_c+3+\|co\|)\|p\|$	$(2n_c+3+\|co\|)\|p\|$
密钥长度	$(2n_c+2)\|p\|$	$(2n_c+2)\|p\|$
用户组总数	$\|m\|$	—
协同通信	$(C_{N_A}^2+\|co\|+1)\|p\|$	$C_{N_A}^2\|p\|$
属性权威	Single	Multiple

表2为本方案与Xue等人[5]提出的属性协同访问控制方案的存储及通信开销对比，且假定文献[5]中的用户属性均来自多个不同的组织。由表2可知，本方案的协同通信效率较同等情况下的协同访问效率要高，且具有近似的密文长度和密钥长度。本方案具有更高的通信效率是由于本方案只需要参与协同的任意两个AA间进行一次通信，即可达到协同的目的，如图3(a)所示。而Xue等人[5]提出的协同方案需要为每次协同建立用户组，如图3(b)所示，可根据协同的先后为参与协同的用户 划分不同类型的用户组，因而系统复杂性更高，协同通信代价更大。

表3 计算开销对比

阶段	Xue[5]	本文方案
CA参数设置	$(5+m)T_e+T_p$	—
AA参数设置	—	$5T_e+T_p$
CA密钥生成	$(2n_u+3)T_e$	—
AA密钥生成	—	$(2n_{a,u}+4)T_e$
加密	$(2n_c+3+\|co\|)T_e$	$(2n_c+3+\|co\|)T_e$
解密	$(2n_{a,u}+2+\|co\|)T_p$ $+(n_{a,u}+\|nl\|)T_e$	$(2n_{a,u}+2+\|co\|)T_p$ $+(n_{a,u}+\|nl\|)T_e$

表3为本方案与文献[5]的计算开销对比，本方案结合单个CA和多个AA的模式，由多个AA负责管理属性和为用户分发私钥，在参数设置和密钥生成阶段进一步减轻了CA的计算负载，在加密、解密阶段具有近似的计算开销，此外AA不再受用户组的限制，进而增强了协同的灵活性、降低了协同的复杂度。

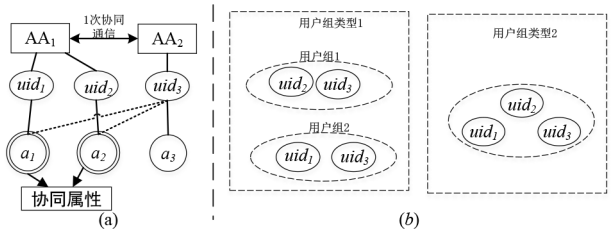

图3 (a)多AA下的协同 (b) 用户组内的协同

7 结束语

本文提出的一种灵活的多权威属性协同访问控制方案，采用单个CA和多AA的属性管理和密钥分发模式，解决了用户属性来源于多属性权威时的协同访问问题。性能分析表明，本方案提供了更灵活的协同访问控制，且更贴合实际需求。所提方案在DBDH困难假设下具有选择明文不可区分性，并能抵抗共谋攻击。

基金项目：

1.国家自然科学基金资助项目（项目编号：U1836205, 61662009, 61772008）；

2.贵州省科技计划项目（项目编号：黔科合重大专项字〔2018〕3001，黔科合支撑（〔2019〕2004，〔2018〕2159），黔科合平台人才〔2020〕5017）；

3.贵州省高等学校创新人才团队（项目编号：黔教合人才团队〔2013〕09）。

参考文献

[1] Sahai A, Waters B. Fuzzy identity-based encryption[C]//24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Aarhus, Denmark, 2005: 457☒473.

[2] Bethencourt J, Sahai A, Waters B. Ciphertext policy attribute-based encryption[C]//IEEE Symposium on Security and Privacy (S&P 2007). Oakland, California, USA ,2007: 321 – 334.

[3] Li Q, Ma J, Li R, et al. Secure, efficient and revocable multi-authority access control system in cloud storage[J]. Computers & Security, 2016, 59(Jun.):45-59.

[4] Federica P, Anna C S, Nicola Z. Survey on access control for community-centered collaborative systems[J]. ACM Computing Surveys, 2018, 51(1): 1-38.

[5] Xue Y J, Xue K P, Gai N, et al. An attribute-based controlled collaborative access control scheme for public cloud storage[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(11): 2927 – 2942.

[6] Xue K P, Chen W K, Li W, et al. Combining data owner-side and cloud-side access control for encrypted cloud storage[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(8): 2062 – 2074.

[7] Waters B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization[C]//International Workshop on Practice and Theory in Public Key Cryptography. Springer, Mar. 2011: 53 – 70.

[8] Shao J, Lu R, Lin X. Fine-grained data sharing in cloud computing for mobile devices[C]//IEEE International Conference on Computer Communications 2015: 2677 – 2685.

[9] Hohenberger S, Waters B. Online/offline attribute-based encryption[C]//International Workshop on Practice and Theory in Public Key Cryptography. Buenos Aires, Argentina: Springer, 2014: 293 – 310.

[10] Humbert M, Trubert B, Huguenin K. A survey on interdependent privacy[J]. ACM Computing Surveys, 2019, 52(6): 1-40.

[11] Willy S, Jiang P, Guo F C, et al. EACSIP: Extendable access control system with integrity protection for enhancing collaboration in the cloud[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(12): 3110-3122.

[12] Li M T, Huang X Y, Josephe K L, et al. GO-ABE: Group-oriented attribute-based encryption[C]//8th International Conference on Network and System Security. Xi'an: Springer, 2014: 260 – 270.

[13] Bobba R, Khurana H, Prabhakaran M. Attribute-sets: A practically motivated enhancement to attribute-based encryption[C]//14th European Conference on Research in Computer Security. Saint-Malo: Springer, 2009: 587 – 604.

[14] Xue K P, Xue Y J, Hong J N, et al. RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(4):

953－967.

[15] Li W, Xue K P, Xue Y J, Et al. TMACS: a robust and verifiable threshold multi-authority access control system in public cloud storage[J]. IEEE Transactions on Parallel and Distributed Systems, 2016, 27(5): 1484－1496.

[16] Chase M. Multi-authority attribute-based encryption[C]//4th Theory Cryptography Conference. 2007: 515－534.

[17] Chase M, Chow S S M. Improving privacy and security in multi-authority attribute-based encryption[C]//16th ACM Conference on Computer Commun-nications Security (CCS). 2009: 121－130.

[18] Müller S, Katzenbeisser S, Eckert C. Distributed attribute-based encryption[C]//11th International Conference on Information Security and Cryptology. Berlin, Germany: Springer, 2009: 20－36.

[19] Lewko A, Waters B. Decentralizing attribute-based encryption[C]// Conference in Advances in European Cryptology. Berlin, Germany: Springer, 2011, pp. 568－588.

[20] Ruj S, Nayak A, and Stojmenovic I. DACC: Distributed access control in clouds[C]//10th International Conference on Trust, Security and Privacy in Computing and Communications. 2011: 91－98.

[21] Beimel A. Secure schemes for secret sharing and key distribution[D]. PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

[22] Diffie W, Hellman M E. New directions in cryptography[J]. IEEE Transactions on Information Theory. 1976, 22(6): 644-654.

作者简介：

彭宗凤（1995-），女，汉族，贵州遵义人，贵州大学，在读硕士；主要研究方向和关注领域：密码学与访问控制。

彭长根（1963-），男，侗族，贵州锦屏人，贵州大学，博士，贵州大学，教授；主要研究方向和关注领域：密码学与信息安全、大数据安全与隐私保护等。

丁红发（1988-），男，汉族，河南南阳人，贵州大学，博士后，贵州财经大学，副教授；主要研究方向和关注领域：数据安全、隐私保护与访问控制。