doi:10.11959/j.issn.1000-436x.2017150

支持树形访问结构的多权威基于属性的签名方案

莫若[1]，马建峰[1]，刘西蒙[2]，李琦[3]
（1. 西安电子科技大学网络与信息安全学院，陕西 西安 710071；2. 新加坡管理大学信息系统学院，新加坡 178902；
3. 南京邮电大学计算机学院、软件学院，江苏 南京 210046）

摘 要：基于属性的签名能够实现细粒度的访问控制，被认为是云计算环境中一种重要的匿名认证手段。但常见的属性基签名只能通过门限结构提供简单的访问控制，无法应对云环境中的大规模用户属性集。同时，用户属性集由唯一的属性权威管理，增加了属性权威的计算和存储开销，一旦属性权威被攻破，整个系统就会面临崩溃的风险。针对以上问题，提出了一种支持树形访问结构的多权威属性签名方案，可以支持任意形式的与、或和门限结构，提供了更灵活的访问控制。将用户属性集由不同属性权威分类管理，减少开销的同时也降低了系统的风险。此外，在随机预言机模型下证明了方案是给定策略选择消息攻击(SP-CMA)安全的。

关键词：基于属性的签名；树形访问结构；多属性权威；随机预言机模型；给定策略选择消息攻击
中图分类号：TP309 **文献标识码**：A

Multi-authority ABS supporting dendritic access structure

MO Ruo[1], MA Jian-feng[1], LIU Xi-meng[2], LI Qi[3]
(1.School of Cyber Engineering, Xidian University, Xi'an 710071, China;
2.School of Information Systems, Singapore Management University, Singapore 178902, Singapore;
3.School of Computer Science and Technology, School of Software, Nanjing University of Posts and Telecommunications, Nanjing 210046, China)

Abstract: Attribute-based signature (ABS), which could realize fine-grained access control, was considered to be an important method for anonymous authentication in cloud computing. However, normal ABS only provided simple access control through threshold structure and thus could not cope with the large-scale attribute sets of users in the cloud. Moreover, the attribute sets were supervised by only one attribute authority, which increased the cost of computation and storage. The whole system was in danger of collapsing once the attribute authority was breached. Aiming at tackling the problems above, a novel scheme, was proposed called multi-authority ABS supporting dendritic access structure which supported any AND, OR and threshold gates and affords more flexible access control. Meanwhile, the attribute sets of users were classified by diverse attribute authorities which reduced the overhead and the risk of systems. Besides, the scheme is proved to be selective predicate chosen message attack secure in the random oracle model.

Key words: attribute-based signature, dendritic access structure, multi-authority, random oracle model, selective predicate chosen message attack

1 引言

云计算在大数据环境下，可以提供共享的计算资源和数据，从而节省用户端的管理开销和计算开销，因此，越来越多的个人和企业开始接触并使用云计算平台，将海量数据上传至第三方云平台保存。但是由于云平台的半可信性，将数据直接暴露在这样的环境下有可能面临被篡改的风险，同时，用户的身份隐私也受到了极大的挑战。因此，如何有效保护数据的完整性和数据拥有者身份的隐私

收稿日期：2016-07-21；**修回日期**：2017-05-10
基金项目：国家自然科学基金资助项目（No.U1135002, No.U1405255）；国家高技术研究发展计划（“863”计划）基金资助项目（No.2015AA016007, No.2015AA017203）
Foundation Items: The National Natural Science Foundation of China (No.U1135002, No.U1405255), The National High Technology Research and Development Program (863 Program) (No.2015AA016007, No.2015AA017203)

性成为了一个重要问题。

基于属性的签名(ABS, attribute based signature)自 2008 年被提出以来，受到了学术界的广泛关注。ABS 首先作为一种数字签名，可以有效防止数据被篡改，保证了数据的完整性； ABS 在传统数字签名的基础上引入了基于属性的访问控制(ABAC, attribute based access control)的概念，将每个签名者的身份信息转化为一系列的属性集，用户仅需声明拥有的属性满足对应的访问结构就可以生成有效的签名，用户的身份信息也不会被公开，从而保证了用户身份的隐私性。因此，ABS 被认为是适用于云计算平台的一种重要匿名认证手段。

在 ABS 中，用户通过唯一的属性权威(AA, attribute authority)生成对应属性的私钥从而生成签名，在云环境中，云服务器扮演着 AA 的角色。但当用户的数量庞大时，单个 AA 需要监管大量的属性，加重了 AA 的计算和存储负担；如果 AA 被敌手攻破，那么整个系统都面临崩溃的风险；在实际生活中，不同类型的属性由一个 AA 存储也是不合理的。例如，身份证号应由公安局管理，驾驶证号应由交通部门管理，职务应由所属的企事业单位管理等。此外，传统 ABS 的门限访问结构只能实现简单的访问控制，无法满足真实的应用需求。针对上述问题，本文提出了一种支持树形访问结构的多权威属性签名方案(DAS-MA-ABS, multi-authority attribute based signature supporting dendritic access structure)，在面对海量数据和用户时可以更好地实现匿名认证，如图 1 所示。本文方案的主要工作可以概括为以下 2 个方面。

1) 把单个 AA 扩展为多个 AA，分担了单个 AA 时所需的存储和计算开销，同时，降低了 AA 被攻破后导致系统崩溃的风险。将门限访问结构改进为树形访问结构，提供更细粒度和灵活的访问控制，使用户的访问权限更加具体。

2) 通过性能分析和安全性证明，本文方案在保证效率的同时满足正确性和匿名性，在随机预言机模型下证明本文方案针对给定策略选择消息攻击(SP-CMA, selective-policy chosen message attack)具有不可伪造性。

2　相关工作

ABS 的概念由基于属性的加密(ABE, attribute based encryption)[1]演变而来，ABE 最早在 2005 年由 Sahai 和 Waters 根据基于身份的加密(IBE, identity based encryption)[2]提出，但是只能支持简单的(t,n)门限结构。为了使访问结构更加灵活，Goyal 等[3]和 Bethencourt 等[4]分别提出了密钥策略 ABE 方案和密文策略 ABE 方案。Chase[5]为了解决上述方案中仅存在一个 AA 的局限性，提出了多权威 ABE(MA-ABE, multi-authority ABE)方案。

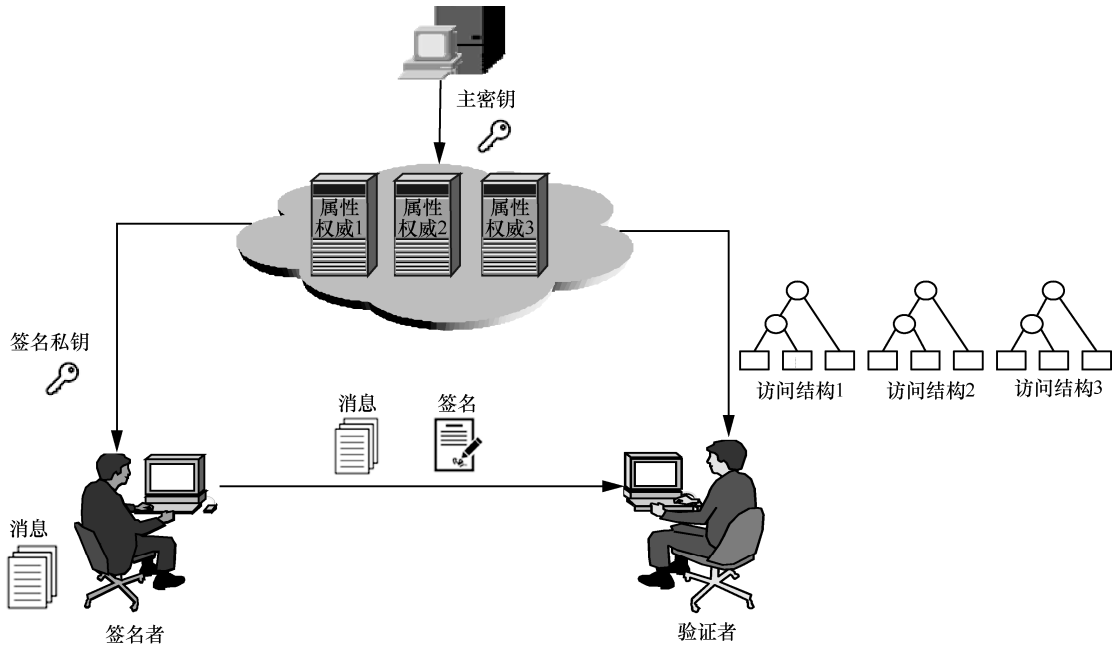

图 1　DAS-MA-ABS 方案示例

Waters[6]在 2005 年根据文献[2]中提到的将加密转换为签名的方法提出了简单的基于身份的签名，为 ABS 的发展打下了基础。Yang 等[7]在 2008 年提出了基于模糊身份的签名方案，即 ABS 的前身，但仅能支持简单的门限结构。Maji 等[8]利用单调张成方案提出了支持灵活访问结构的 ABS 方案，但是只在一般群模型下证明了方案的安全性。Li 等[9]在 2010 年提出了一种 ABS 方案并在标准模型下证明了方案是安全的。Su 等[10]基于计算性 Diffie-Hellman (CDH, computational Diffie-Hellman) 困难假设提出了一种支持灵活访问结构的 ABS 方案。为了解决单一 AA 的问题，Li 等[11]在 2015 年提出了一种多权威的 ABS 方案，并证明了方案的不可伪造性。

3 预备知识

本节给出所提方案中所需要用到的预备知识：CDH 困难性假设和访问结构的定义。

3.1 CDH 困难性假设

假设 g 是 $\mathbb{G}_1$ 的生成元，对 $a,b\leftarrow\mathbb{Z}_p^*$，在给出 g、g^a、g^b 的前提下计算 g^{ab}，称之为 CDH 问题。如果不存在多项式时间的敌手在 t 时间内能以不可忽略的概率 ε 解决 CDH 问题，称 (t,ε)−CDH 假设成立。

3.2 访问结构

用 $\Lambda=\{P_1,P_2,\cdots,P_n\}$ 表示参与方的集合。对一个访问结构 $\mathbb{A}\subseteq 2^{\{P_1,P_2,\cdots,P_n\}}$，$\forall B,C$，如果 $B\in\mathbb{A}$ 且 $B\subseteq C$ 则有 $C\in\mathbb{A}$，则称 $\mathbb{A}$ 是单调的。$\mathbb{A}$ 中的集合称作授权集合，不在 $\mathbb{A}$ 中的集合称为非授权集合。

在本文方案中，用属性代替参与方的角色。因此，访问结构 $\mathbb{A}$ 将包含授权的属性。门限访问结构由一个门限和多个属性组成。叶子节点表示访问结构中的属性集 ω^*，根节点表示门限，仅当用户的属性 ω 和访问结构中属性 ω^* 的交集不小于门限值 t 时有 $\Gamma_{t,\omega^*}(\omega)=1$，即该用户可以生成有效的签名。

树形访问结构是多个门限结构的组合。叶子节点表示访问结构中的属性集 ω^*，根节点和内部节点都表示门限。对任意节点 x，定义函数 $parent(x)$ 表示其父节点。对同父节点的所有节点列出索引，函数 $index(x)$ 表示 x 节点在其他同父节点中的索引值。

门限访问结构只能实现简单的访问控制，如“$A\cap B\cap C$”或“$A\cup B\cup C$”，而通过树形访问结构除了可以定义上述访问策略外，还可定义“$(A\cap B)\cup C$”和“$(A\cup B)\cap C$”等访问策略。在大规模属性集中，通过改变树形访问结构的深度和广度，可以提供更为灵活的访问控制，使用户的访问权限更加具体。

4 DAS-MA-ABS 方案

本节给出 DAS-MA-ABS 方案的系统模型和具体算法设计。

4.1 DAS-MA-ABS 系统模型

DAS-MA-ABS 方案包括 2 类个体：若干属性权威 $A_1,A_2,\cdots,A_k$ 和用户 U。用 $\mathbb{A}=\{\mathbb{A}_k\}_{k\in\{1,2,\cdots,N\}}$ 表示所有的属性组成的集合，权威 A_k 定义访问结构 Γ_k，其中包含属性集合 $\mathbb{A}_k$，不同权威中的属性集合互不相交。用户 U 包含来自各个权威中的属性，并且可以通过属性权威获得对应的属性私钥。

DAS-MA-ABS 方案由初始化、密钥生成、签名、验证 4 部分组成。

1) 初始化 $Setup(\lambda,N)\rightarrow(params,\{Mk_k\}_{k\in\{1,2,\cdots,N\}})$：*Setup* 算法输入一个安全参数 λ，属性权威个数 N，输出系统的公开参数 *params* 和属性权威的主密钥 $\{Mk_k\}_{k\in\{1,2,\cdots,N\}}$。

2) 属性签名私钥生成 $UsersignkeyGen(Mk_k,GID,\mathbb{A}_k)\rightarrow Usk_k[GID,\mathbb{A}_k]$：属性权威 A_k 调用 *UsersignkeyGen* 算法，输入主密钥 Mk_k，输出身份为 *GID* 的用户属性签名私钥 Usk_k。

3) 验证公钥生成 $VerikeyGen(\Gamma_k,Mk_k)\rightarrow Vk_k$：*VerikeyGen* 算法输入访问结构 Γ_k 和主密钥 Mk_k，输出关于访问策略的公钥 Vk_k。

4) 签名 $Sign(\{\Gamma_{\mathbb{P}_k},Usk_k[GID,\mathbb{A}_k]\}_{k\in\{1,2,\ldots,N\}},M)\rightarrow\sigma$：$\Gamma_{\mathbb{P}_k}$ 表示所有属性权威的访问结构，*Sign* 算法利用用户的属性签名私钥 Usk_k 生成对消息 M 的签名 σ。

5) 验证 $Verify(Vk,params,M,\sigma)\rightarrow 1/0$：*Verify* 算法验证用户的属性是否满足访问结构，如果满足则证明改签名有效，输出 1；否则输出 0。

4.2 DAS-MA-ABS 方案设计

在支持门限结构的单权威属性签名方案[7]中，

只有在用户的属性集和访问结构 Γ 中属性集的交集大于门限值时，用户才可以生成有效的签名。而在 DAS-MA-ABS 方案中存在多个属性权威，且每个属性权威都会定义各自的树形访问结构，只有当用户属性集同时满足每个属性权威中的访问结构时，才能生成有效的签名。

1) 初始化。给定 2 个 p 阶循环乘法群 $\mathbb{G}_1$、$\mathbb{G}_2$，p 是一个大素数，$g \in \mathbb{G}_1$ 是 $\mathbb{G}_1$ 的生成元；同时，定义 $g_2 \in \mathbb{G}_1$；定义双线性映射 $e:\mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ 和 2 个散列函数 $H_1, H_2:\{0,1\}^* \to \mathbb{G}_1$。对每个属性权威 A_k，选取 $x_k \in \mathbb{Z}_p$ 为每个属性权威的主密钥 msk_k 并计算 $g_{1_k} = g^{x_k}$。$T_k = e(g_{1_k}, g_2)$ 为每个属性权威 A_k 的公钥 gpk_k，$T = \prod_{k=1}^{N} T_k$ 为系统的总公钥。

2) 属性签名私钥生成。由于用户必须向每个属性权威提交同一个 *GID* 获取签名私钥，那么属性权威可以通过共谋的手段恢复出 *GID* 的部分属性。为了防止上述情况发生，本文采用文献[12]中的密钥分发协议。

属性权威 A_k 向其他属性权威 A_j 共享一个伪随机函数种子 s_{kj}，令 $s_{kj} = s_{jk}$。A_k 定义伪随机函数种子 $a_k \in \mathbb{Z}_p^*$，计算 $y_k = g_2^{a_k}$ 并发送至其余的属性权威。如果用户 A 将自己的属性私钥交给用户 B，那么 B 可以将自己的私钥和 A 的私钥组合伪造他人的签名从而实现共谋攻击。因此，给予每个用户一个全局标识符 *GID* 并定义伪随机函数 $PRF_{kj}(GID) = g_2^{\frac{a_k a_j}{s_{kj}+GID}}$。

为了获得 A_k 中相关属性的属性私钥，用户通过密钥分发协议获得 $\{D_{kj} \mid j \neq k\} = \begin{cases} g_2^{R_{kj}} PRF_{kj}(GID), k > j \\ \dfrac{g_2^{R_{kj}}}{PRF_{kj}(GID)}, k < j \end{cases}$，其中，$R_{kj} \in \mathbb{Z}_p^*$。根据 D_{kj}，用户计算 $D = \prod_{\substack{(k,j)\in\{1,\cdots,N\}\times \\ (\{1,\cdots,N\}\setminus\{k\})}} D_{kj} = g_2^R$，$R = \sum_{\substack{k,j\in\{1,2,\cdots,N\}\times \\ \{\{1,2,\cdots,N\}\setminus\{k\}\}}} R_{kj}$。对每个属性权威 A_k，令 $X_k = x_k - \sum_{j\in\{1,2,\cdots,N\}\setminus\{k\}} R_{kj}$ 选取 $r_k \in \mathbb{Z}_p^*$ 并计算 $d_k = g_2^{r_k + X_k}$。对每个用户的属性 $i \in \mathbb{A}_k$ 计算 $d_{ki0} = g_2^{\frac{r_k}{X_k}} H_1(i)^{r_i}, d_{ki1} = g^{r_i}$。每个权威中的签名密钥为 $sk_{ki} = \left(d_k, \{d_{ki0}, d_{ki1}\}_{i\in\mathbb{A}_k}\right)$。

3）验证公钥生成。对 A_k 中树形访问结构 Γ_k 中的每个节点 y_k 设计阶为 $t_{y_k} - 1$ 的多项式 $q_{y_k}(\cdot)$，t_{y_k} 是每个节点的门限值。本文采用自顶向下的方式对树形访问结构进行构造，首先定义根节点 $q_{root_k}(0) = X_k$，其次对根节点的每个子节点 y_k 定义 $q_{y_k}(0) = q_{parent(y_k)}\left(index\left(y_k\right)\right)$，最后对所有的叶子节点 y_k 和 $i = attr(y_k)$ 计算 $h_i = H_1(i)^{q_{y_k}(0)}, D_{y_k} = g^{q_{y_k}(0)}$。

4) 签名。用 $\mathbb{A}_k^*$ 表示树形访问结构 Γ_k 中包含的所有叶子节点的集合，对消息 $M = m_1 m_2 \cdots m_n$，选取 $u, u_1, u_2, \cdots, u_n \in \mathbb{G}_1$，计算 $u\prod_{i=1}^{n} u_i^{m_i}$。随机选取 $s \in \mathbb{Z}_p^*$，计算

$$\sigma_0 = d(u\prod_{i=1}^{n} u_i^{m_i})^s D, \sigma_0' = g^s$$

其中，$d = \prod_{k=1}^{N} d_k$。

对每个属性权威 A_k，随机选择 $r_i' \in \mathbb{Z}_p^*$ 并分别计算

$$\{\sigma_{ki0} = d_{ki0} H_1(i)^{r_i'}, \sigma_{ki1} = d_{ki1} g^{r_i'}\}_{i\in\mathbb{A}_k \cap \mathbb{A}_k^*}$$
$$\{\sigma_{ki0} = H_1(i)^{r_i'}, \sigma_{ki1} = g^{r_i'}\}_{i\in\mathbb{A}_k^* \setminus \mathbb{A}_k \cap \mathbb{A}_k^*}$$

最终生成的签名为 $\sigma = (\sigma_0, \{\sigma_{ki0}, \sigma_{ki1}\}_{i\in\mathbb{A}_k^*}, \sigma_0')$。

5) 验证。首先定义递归函数 $Vernode(\sigma, Vk, y_k)$，在权威 A_k 中，对每个叶子节点 y_k 计算 $\dfrac{e(\sigma_{ki0}, D_{y_k})}{e(\sigma_{ki1}, h_i)}$。

当 $i \in \mathbb{A}_k \cap \mathbb{A}_k^*$ 时，有

$$\frac{e(\sigma_{ki0}, D_{y_k})}{e(\sigma_{ki1}, h_i)} = \frac{e(g_2^{\frac{r_k}{X_k}} H_1(i)^{r_i} H_1(i)^{r_i'}, g^{q_{y_k}(0)})}{e(g^{r_i} g^{r_i'}, H_1(i)^{q_{y_k}(0)})} = e(g, g_2)^{q_{y_k}(0)}$$

当 $i \in \mathbb{A}_k^* \setminus \mathbb{A}_k \cap \mathbb{A}_k^*$ 时，有

$$\frac{e(\sigma_{ki0}, D_{y_k})}{e(\sigma_{ki1}, h_i)} = \frac{e(H_1(i)^{r_i'}, g^{q_{y_k}(0)})}{e(g^{r_i'}, H_1(i)^{q_{y_k}(0)})} = 1$$

对每个非叶子节点 z_k，首先计算其子节点 y_k 的 $Vernode(\sigma, Vk, y_k)$ 值并将其命名为 F_{y_k}，定义一个大

小为 t_{z_k} 的集合 S_{z_k} 表示其所有子节点并计算

$$\begin{aligned}F_{z_k} &= \prod_{y_k \in S_{z_k}} F_{y_k}^{\Delta i, S_{z_k}(0)} \\ &= \prod_{y_k \in S_{z_k}} (e(g,g_2)^{q_{y_k}(0)\frac{r_k}{X_k}})^{\Delta i, S_{z_k}(0)} \\ &= \prod_{y_k \in S_{z_k}} (e(g,g_2)^{q_{parent(y_k)}(index(y_k))\frac{r_k}{X_k}})^{\Delta i, S_{z_k}(0)} \\ &= \prod_{y_k \in S_{z_k}} e(g,g_2)^{q_{z_k}(i)\frac{r_k}{X_k}\Delta i, S_{z_k}(0)} \\ &= e(g,g_2)^{q_z(0)\frac{r_k}{X_k}}\end{aligned}$$

因此，$F_{root_k} = e(g,g_2)^{r_k}$。在得出 F_{root_k} 值后，计算 $\dfrac{e(g,\sigma_0)}{\prod_{k=1}^{N} F_{root_k} e(u\prod_{i=1}^{n} u_i^{m_i}, \sigma_0^{'})} \overset{?}{=} T$，如果相等，则证明该签名有效；否则声明该签名无效。

5 DAS-MA-ABS 方案分析

本节通过安全性证明给出 DAS-MA-ABS 方案的正确性、匿名性和不可伪造性的证明，并通过对比给出了方案的性能分析。

5.1 方案证明

定义 1 （正确性）。如果对于所有符合访问结构 $\Gamma_{\mathbb{P}_k}$ 的用户 U，都可以生成有效的签名，即 $Verify(Vk, params, M, Sign(\{\Gamma_{\mathbb{P}_k}, Usk_k[GID, \mathbb{A}_k]\}_{k\in\{1,2,\cdots,N\}}, M)) \to 1$，那么 DAS-MA-ABS 方案满足正确性。

定理 1 本文方案具有正确性。

证明 如果用于生成签名的所有属性可以满足对应属性权威中的访问结构，那么可以计算出访问结构 Γ_k 的 $F_{root_k} = e(g,g_2)^{r_k}$。因此，有

$$\begin{aligned}&\frac{e(g,\sigma_0)}{\prod_{k=1}^{N} F_{root_k} e(u\prod_{i=1}^{n} u_i^{m_i}, \sigma_0')} \\ &= \frac{e(g, \prod_{k=1}^{N} g_2^{r_k+X_k}) e(g, (u\prod_{i=1}^{n} u_i^{m_i})^s) e(g, g_2^R)}{\prod_{k=1}^{N} e(g,g_2)^{r_k} e(u\prod_{i=1}^{n} u_i^{m_i}, g^s)} \\ &= \frac{e(g,g_2)^{R+\sum_{k=1}^{N}(r_k+X_k)}}{e(g,g_2)^{\sum_{k=1}^{N} r_k}} \\ &= e(g,g_2)^{R+X} = \prod_{k=1}^{N} e(g_{1_k}, g_2) = T\end{aligned}$$

定义 2 （匿名性）。匿名性是指任何一名用户，如果具有满足访问结构的属性，即 $\Gamma(\omega)=1$，那么他在所有具备这样条件的用户中是匿名的，这样的用户生成的签名和其他满足访问结构的用户生成的签名具有同样的分布，敌手无法根据签名判断签名者的身份。本文假设敌手 $\mathcal{A}$ 和挑战者 $\mathcal{C}$，通过如下游戏给出匿名性的形式化定义。

1) 初始化。挑战者 $\mathcal{C}$ 选择安全参数 λ，运行 *Setup* 函数，得到主密钥 *Mk* 和公开参数 *params* 并交给敌手 $\mathcal{A}$。

2) 属性选择。$\mathcal{A}$ 选择消息 M^* 和 2 个满足访问结构 Γ 的属性集 ω_0、ω_1，利用 *Mk* 分别计算 2 个属性集的属性签名私钥 sk_{ω_0}、sk_{ω_1} 然后交给 $\mathcal{C}$。

3) 挑战。$\mathcal{C}$ 随机选择一个比特 $b \in \{0,1\}$，计算签名 $\sigma^* = Sign(\Gamma, M^*, sk_{\omega_b})$，将 σ^* 交还给 $\mathcal{A}$，由 $\mathcal{A}$ 判断该签名来自 ω_0 还是 ω_1。

4) 竞猜。$\mathcal{A}$ 输出一个比特 b'，如果 $b=b'$ 则称敌手赢得游戏。

定义敌手在上述安全游戏里的优势 $Adv^{\text{anony}}_{\text{DAS-MA-ABS},\mathcal{A}} = \left|\Pr[b=b'] - \frac{1}{2}\right|$。如果没有敌手 $\mathcal{A}$ 能以不可忽略的优势赢得上述游戏，则称 DAS-MA-ABS 方案满足匿名性。

定理 2 本文方案具有匿名性。

证明 在 DAS-MA-ABS 方案中，签名本身并不会泄露到底是哪些属性生成的签名，因为任何一个满足访问结构的属性集 $\mathbb{A}$ 都可以生成有效的签名。因此，只需要证明即便在 $\mathbb{A}=\mathbb{A}^*$ 的条件下，拥有这些属性的用户在所有这样的用户中仍然具备匿名性即可，$\mathbb{A}^*$ 是访问结构 Γ 中的叶子属性节点。

运行 *Setup* 算法，获得公开参数 *params* 和主密钥 X，并交给敌手 $\mathcal{A}$。$\mathcal{A}$ 选择 2 个满足访问结构 Γ 的属性集 $\mathbb{A}_1$ 和 $\mathbb{A}_2$，计算 $sk_{\mathbb{A}_1} = \left(d^1, \left\{d_{i0}^1, d_{i1}^1\right\}_{i\in\mathbb{A}_1}\right)$ 和 $sk_{\mathbb{A}_2} = \left(d^2, \left\{d_{i0}^2, d_{i1}^2\right\}_{i\in\mathbb{A}_2}\right)$。对每个属性 $i \in \mathbb{A}_\theta$，令 $d^\theta = g_2^{r_\theta + X}, d_{i0}^\theta = g_2^{\frac{r_\theta}{X}} H_1(i)^{r_i^\theta}, d_{i1}^\theta = g^{r_i^\theta}$，其中，$\theta \in \{1,2\}$，$r_\theta, r_i^\theta \in \mathbb{Z}_p$。$\mathcal{A}$ 将属性签名私钥交给 $\mathcal{C}$。

$\mathcal{C}$ 随机选择一个比特 $b \in \{1,2\}$ 和消息 M^*，通过

Sign 算法计算签名 $\sigma^*=(g_2^{r+X}(u\prod_{i=1}^{n}u_i^{m_i^*})^s D,\{\sigma_{i0}=g_2^{\frac{r}{X}}H_1(i)^{r_i},\sigma_{i1}=g^{r_i}\}_{i\in\mathcal{A}^*},g^s)$，很明显，这个签名可能由 $sk_{\mathcal{A}_1}$ 和 $sk_{\mathcal{A}_2}$ 中任何一个生成。因此，如果一个签名来自于属性集 $\mathcal{A}_1$ 的签名私钥 $sk_{\mathcal{A}_1}$，那么它也可能来自于属性集 $\mathcal{A}_2$ 的签名私钥 $sk_{\mathcal{A}_2}$。综上，本文方案具有匿名性。

定义 3（不可伪造性）。如果没有多项式时间的敌手 $\mathcal{A}$ 能够在最多 t 时间内，通过 q_k 次属性私钥查询和 q_s 次签名查询以不小于 ε 的优势 $Adv^{\mathrm{UF}}_{\text{DAS-MA-ABS},\mathcal{A}}$ 攻破 DAS-MA-ABS 方案，称 DAS-MA-ABS 方案是 (t,q_k,q_s,ε)-不可伪造的。

在本文方案中，考虑了一种较 CMA 稍弱的攻击模型，即 SP-CMA 模型[9]，敌手在初始化之前需要预先选择挑战访问策略 Γ^*。本文假设敌手 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 并通过如下游戏给出不可伪造性的形式化定义。

1) 初始化。$\mathcal{A}$ 选择在伪造签名阶段即将用到的挑战访问策略 Γ^*。挑战者 $\mathcal{C}$ 选择安全参数 λ，调用 *Setup* 函数，生成主密钥 *msk* 和公开参数 *params*，将 *params* 交给 $\mathcal{A}$。

2) 属性签名私钥查询。在收到公开参数后，$\mathcal{A}$ 可以对属性集 ω 向属性私钥生成预言机进行多项式次的属性私钥生成查询，预言机生成对应的属性私钥 sk_ω 并交给 $\mathcal{A}$。

3) 签名查询。收到属性私钥后，$\mathcal{A}$ 向签名预言机提交多项式次的消息和访问结构 (M,Γ) 询问，签名预言机计算对应的签名 σ，交给敌手 $\mathcal{A}$。

4) 伪造。最终 $\mathcal{A}$ 输出消息 M^* 和访问结构 Γ^* 的签名 σ^*，Γ^* 是 $\mathcal{A}$ 在初始化阶段定义的挑战访问策略。

如果 σ^* 是 (M^*,Γ^*) 的有效签名，且 (M^*,Γ^*) 在签名查询中未曾被查询，且任何满足挑战访问策略 Γ^* 的属性集 ω^* 都未曾出现在属性签名私钥查询中，则称敌手 $\mathcal{A}$ 赢得游戏。敌手的优势定义为 $\left|\Pr\left[Verify(\sigma^*,M^*,\Gamma^*)=1\right]\right|$，如果该优势是可忽略的，那么称该方案具有不可伪造性。

定理 3　假设敌手 $\mathcal{A}$ 能够在最多进行 q_{H_1} 次 $H_1(\cdot)$ 随机预言机查询、q_k 次属性私钥查询和 q_s 次签名查询的前提下，在时间 t 内以 ε 的概率攻破该签名方案，那么存在算法 $\mathcal{B}$ 在时间 $t'<t+(q_{H_1}+2q_k+5q_s)t_{\exp}$ 内，以 $\varepsilon'\geqslant\frac{\varepsilon}{4(n+1)q_s}$ 的概率攻破 CDH 问题，其中，$t_{\exp}$ 表示在 $\mathbb{G}_1$ 中进行幂运算的最大时间。

证明　假设存在敌手 $\mathcal{A}$ 具有优势攻破本文的签名方案，那么可以构造一个算法 $\mathcal{B}$ 利用 $\mathcal{A}$ 解决 CDH 问题，即在给定 $g,g^x,g^y\in\mathbb{G}_1$ 的情况下计算 g^{xy}。

1) 初始化阶段

$\mathcal{A}$ 对每个属性权威定义访问策略即树形访问结构 Γ^*，用 $\mathbb{A}^*$ 表示访问结构中所有的属性集合，$\mathcal{B}$ 获得 $g_1=g^x,g_2=g^y$。假设 $\mathcal{A}$ 最多可以对随机预言机 $H_1(\cdot)$ 进行 q_{H_1} 次查询，定义 $\mathcal{C}$ 维护 H_1 预言机的列表 L_1 并存储散列值。如果访问结果可以在 L_1 中找到，那么直接将结果反馈给敌手 $\mathcal{A}$；否则，通过如下方式进行模拟。

① 如果 $i\in\mathbb{A}^*$，随机选择 $\beta_i\in\mathbb{Z}_p$，计算 $H_1(i)=g^{\beta_i}$。

② 如果 $i\notin\mathbb{A}^*$，随机选择 $\beta_i,\gamma_i\in\mathbb{Z}_p$，计算 $H_1(i)=g_1^{-\beta_i}g^{\gamma_i}$。

2) 私钥生成阶段

$\mathcal{A}$ 可以对所有满足 $\Gamma^*(\mathbb{A})\neq1$ 的属性集 $\mathbb{A}$ 进行最多 q_k 次私钥生成查询。因为 $\Gamma^*(\mathbb{A})\neq1,\mathbb{A}\cap\mathbb{A}^*\subseteq\mathbb{A}$，所以 $\Gamma^*(\mathbb{A}\cap\mathbb{A}^*)\neq1$。定义可以满足访问结构 Γ^* 的属性集合 $\mathbb{S}$，且 $\mathbb{A}\cap\mathbb{A}^*\subseteq\mathbb{S}$，随机选择 $R,r\in\mathbb{Z}_p^*$，令 $X=x-R$，计算 $d=g_2^{r+X}$，并对 d_{i0}、d_{i1} 进行模拟。

① 如果 $i\in\mathbb{S}$，选择 $r_i\in\mathbb{Z}_p$，计算 $d_{i0}=g_2^{\frac{r}{X}}H_1(i)^{r_i},d_{i1}=g^{r_i}$。

② 如果 $i\notin\mathbb{S}$，选择 $r_i'\in\mathbb{Z}_p$，计算 $d_{i0}=g_2^{\frac{r}{X}+\Delta0,s(i)\frac{\gamma_i}{\beta_i}}g^{-y/X\Delta0,s(i)}(g_1^{-\beta_i}g^{\gamma_i})^{r_i'},d_{i1}=g_2^{\frac{\Delta0,s(i)}{\beta_i}}g^{r_i'}$。

由于令 $r_i=\beta\Delta0,\frac{s(i)}{\beta_i}+r_i'$，因此上述模拟正确。

3) 公钥生成阶段

对访问结构 Γ^* 中的每个节点，随机选择任意阶多项式 $q(\cdot)$ 并采用自顶向下的方式赋值，令 $q_{root}(0)=X$，其余节点 y 令 $q_y(0)=q_{parent(y)}(index(y))$。

4) 签名阶段

假设敌手 $\mathcal{A}$ 可以进行 q_s 次签名查询，定义 $l=2q_s$。$\mathcal{B}$ 随机选择整数 k，满足 $0\leqslant k\leqslant n$，n 为消息 M 的长度。同时，假设对于给定的 q_s 和 n，有 $l(n+1)<p$。随机选择

① $x' \in \mathbb{Z}_l, y' \in \mathbb{Z}_p$

② $x_i \in \mathbb{Z}_l, y_i \in \mathbb{Z}_p, 1 \leqslant i \leqslant n$

对 M 定义函数：$F(M)=x'+\sum_{i=1}^{n} x_i m_i - lk$, $J(M)=y'+\sum_{i=1}^{n} y_i m_i$。$\mathcal{B}$ 构造 $u=g_2^{-lj+x'} g^{y'}, u_i=g_2^{x_i} g^{y_i}, i=1,\cdots,n$，可以得到 $u\prod_{i=1}^{n} u_i^{m_i}=g_2^{F(M)} g^{J(M)}$。

$\mathcal{B}$ 根据 $\mathcal{A}$ 第 j 次对 M_j 的签名请求，计算

$$\begin{aligned}\sigma_0 &= g^{\frac{-rJ(M_j)}{F(M_j)}} g_1^{\frac{-J(M_j)}{F(M_j)}} (g_2^{F(M_j)} g^{J(M_j)})^s \\ &= g^{\frac{-(x+r)J(M_j)}{F(M_j)}} (g_2^{F(M_j)} g^{J(M_j)})^{\frac{x+r}{F(M_j)}} \cdot \\ &\quad (g_2^{F(M_j)} g^{J(M_j)})^{\frac{-(x+r)}{F(M_j)}} (g_2^{F(M_j)} g^{J(M_j)})^s \\ &= g_2^{x+r} (g_2^{F(M_j)} g^{J(M_j)})^{s-\frac{(x+r)}{F(M_j)}} \\ \sigma_0' &= g^{\frac{-r}{F(M_j)}} g_1^{\frac{-1}{F(M_j)}} g^s\end{aligned}$$

令 $s'=s-\frac{(x+r)}{F(M_j)}, D=g_2^R$，可以得到：$\sigma_0=g_2^{X+r}(g_2^{F(M_j)} g^{J(M_j)})^{s'} D, \sigma_0'=g^{s'}$。

如果 $F(M_j)=0 \bmod p$，上述计算过程无法进行，模拟中止。

根据假设 $l(n+1)<p$，因为 $0 \leqslant k \leqslant n$，所以有 $0 \leqslant lk < p$；又因为 $x'<l, x_i<l$，所以 $0 \leqslant x'+\sum_{i=1}^{n} x_i m_i < p$。综上，可以求得 $-p<F(M_j)<p$，因此，如果 $F(M_j)=0 \bmod p$，就有 $F(M_j)=0 \bmod l$；相反，如果 $F(M_j) \neq 0 \bmod l$，那么 $F(M_j) \neq 0 \bmod p$。因此，只要满足 $F(M_j) \neq 0 \bmod l$ 就可以继续模拟。

5) 挑战阶段

如果上述阶段不中止，$\mathcal{A}$ 可以生成新消息 M^* 的签名 $\sigma_0^*=g_2^{X+r}(g^{J(M^*)})^{s^*} D, \{\sigma_{i0}^*=g_2^{\frac{r}{X}} H_1(i)^{r_i}, \ \sigma_{i1}^*=g^{r_i}\}_{i \in A^*}$ $\sigma_0'^{\,*}=g^{s^*}$，如果 $F(M^*) \neq 0 \bmod p$，则模拟中止。

$\mathcal{B}$ 模拟递归函数 $ReNode(y, \Gamma^*)$。如果 y 是 Γ^* 中一个叶子节点，即属性节点 i，那么 $H_1(i)=g^{\beta_i}$，则有 $ReNode(y,\Gamma^*)=\left(\frac{(\sigma_{i1}^*)^{\beta_i}}{(\sigma_{i0}^*)}\right)^{q_y(0)}=g_2^{\frac{q_y(0)\cdot(-r)}{X}}$。对非叶子节点 z，计算其子节点 y 的 $ReNode(y,\Gamma^*)$ 值并记为 R_y。定义一个大小为 K_z 的集合 S_z 存储子节点 y，并计算

$$\begin{aligned}R_z &= \prod_{y \in S_z} R_y^{\Delta i, S_z(0)} = \prod_{y \in S_z} g_2^{-\frac{r}{X} \cdot q_y(0) \Delta i, S_z(0)} \\ &= \prod_{y \in S_z} g_2^{-\frac{r}{X} q_{parent(y)}(index(y)) \Delta i, S_z(0)} \\ &= \prod_{y \in S_z} g_2^{-\frac{r}{X} q_z(i) \Delta i, S_z(0)} \\ &= g_2^{-\frac{r}{X} q_z(0)}\end{aligned}$$

因此，$R_{\text{root}}=g_2^{-r}$。可以求得 $R_{\text{root}} \frac{\sigma_0^*}{(\sigma_0'^{\,*})^{J(M^*)}}=g_2^{x+r} g_2^{-r}=g^{xy}$。

6) 不中止概率

模拟的顺利运行取决于如下 2 个事件。

① 对于 q_s 次的签名查询总有 $F(M_j) \neq 0 \bmod l$，命名为事件 A_j。

② 挑战阶段的 $F(M^*)=0 \bmod p$，命名为事件 A^*。

$\mathcal{B}$ 的不中止概率 $\Pr[\overline{abort}]=\Pr\left[\bigcap_{j=1}^{q_s} A_j \cap A^*\right]$。由于 $0<x'<l, 0<x_i<l$，那么 $0<x'+\sum_{i=1}^{n} x_i m_i^* < l(n+1)$，因此，$0 \leqslant F(M^*) \bmod p < l(n+1)$，得出 $\Pr[A^*]=\frac{1}{l(n+1)}$，同理可求得 $\Pr[\neg A_j]=\frac{1}{l}$。因为事件 A_j 和 A^* 相互独立，可以得到

$$\begin{aligned}\Pr\left[\bigcap_{j=1}^{q_s} A_j \cap A^*\right] &= \Pr[A^*] \Pr\left[\bigcap_{j=1}^{q_s} A_j \mid A^*\right] \\ &= \frac{1}{l(n+1)} \Pr\left[\bigcap_{j=1}^{q_s} A_j \mid A^*\right] \\ &\geqslant \frac{1}{l(n+1)} \left(1-\sum_{j=1}^{q_s} \Pr[\neg A_j \mid A^*]\right) \\ &\geqslant \frac{1}{4(n+1)q_s}\end{aligned}$$

因此，解决 CDH 问题的概率为 $\varepsilon' \geqslant \frac{\varepsilon}{4(n+1)q_s}$。

5.2 性能分析

表 1 给出了 DAS-MA-ABS 方案的效率分析，其中，k 表示属性权威的个数，ω 表示用户的属性，l 表示每个权威的访问结构中包含的属性，m 表示消息的长度，τ 表示集合 S_{z_k} 中元素的个数，在门限结构属性签名方案[9,11]中，d 为门限值。P 和 EXP 分别表示方案中双线性对和幂运算的次

表 1　　**方案效率比较**

参数	本文方案	文献[9]方案	文献[10]方案	文献[11]方案
公开参数 *params*	$(k+2)\lvert\mathbb{G}_1\rvert+k\lvert\mathbb{G}_2\rvert$	$3\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert$	$3\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert$	$\lvert\mathbb{G}_1\rvert+k\lvert\mathbb{G}_2\rvert$
主密钥 *Mk*	$k\lvert\mathbb{Z}_p\rvert$	$\lvert\mathbb{Z}_p\rvert$	$\lvert\mathbb{Z}_p\rvert$	$k\lvert\mathbb{Z}_p\rvert$
签名私钥 *Usk*	$(2\omega+k)\lvert\mathbb{G}_1\rvert$	$(2\omega+1)\lvert\mathbb{G}_1\rvert$	$(2\omega+1)\lvert\mathbb{G}_1\rvert$	$(2\omega+1)\lvert\mathbb{G}_1\rvert$
验证公钥 *Vk*	$2kl\lvert\mathbb{G}_1\rvert$	—	$2l\lvert\mathbb{G}_1\rvert$	—
签名长度	$(2kl+2)\lvert\mathbb{G}_1\rvert$	$(kl+2)\lvert\mathbb{G}_1\rvert$	$(2l+2)\lvert\mathbb{G}_1\rvert$	$(kl+2)\lvert\mathbb{G}_1\rvert$
签名生成开销	$(2kl+m+2)EXP$	$(2kl+kd+2)EXP$	$(2l+2)EXP$	$(2kl+kd+2)EXP$
验证开销	$2klP+k\tau EXP$	$(kl+2)P$	$2lP+\tau EXP$	$(kl+2)P$

数。通过和现有方案对比，本文方案在公开参数、主密钥、签名私钥长度以及签名生成开销方面与现有多权威属性签名方案[9,11]相当。在 DAS-MA-ABS 中，由于需要利用额外生成的签名 σ_{ki0}、σ_{ki1} 在验证过程中通过递归求出树形访问结构的 $q_{root_k}(0)$，因此，方案的签名长度和验证开销略长于现有方案。

表 2 给出了 DAS-MA-ABS 方案与现有方案在功能上的对比。本文方案在提供了细粒度访问控制，保证匿名性的同时，支持树形访问结构，提供了更为灵活的访问控制，同时支持多属性权威，降低了系统开销和风险。

6　结束语

为了减少属性签名中单一属性权威计算开销，降低系统风险，同时，在大数据环境中提供灵活的访问控制，本文提出了一种支持树形访问结构的多属性权威 ABS 方案。安全性分析表明，本文方案满足正确性和匿名性，在随机预言机模型下具有不可伪造性。通过与和现有方案对比，本文方案在降低权威计算开销和系统风险的同时，支持树形访问结构，可以在大规模属性集中提供灵活的访问控制。

参考文献：

[1] SAHAI A, WATERS B. Fuzzy identity-based encryption[M]. Advances in Cryptology–EUROCRYPT 2005. Springer Berlin Heidelberg, 2005: 457-473.

[2] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[C]//Annual International Cryptology Conference. Springer Berlin Heidelberg, 2001: 213-229.

[3] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//The 13th ACM Conference on Computer and Communications Security. ACM, 2006: 89-98.

[4] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//IEEE Symposium on Security and Privacy. Computer Society, 2007: 321-334.

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

[6] WATERS B. Efficient identity-based encryption without random oracles[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg. 2005: 114-127.

表 2　　**方案功能比较**

功能	本文方案	文献[9]方案	文献[10]方案	文献[11]方案
细粒度访问控制	是	是	是	是
匿名性	是	是	是	是
树形访问结构	是	否	是	否
多属性权威	是	是	否	是
安全模型	随机预言机模型	随机预言机模型	随机预言机模型	随机预言机模型

[7] YANG P, CAO Z, DONG X. Fuzzy identity based signature[J]. IACR Cryptology ePrint Archive, 2008: 2.

[8] MAJI H K, PRABHAKARAN M, ROSULEK M. Attribute-based signatures[C]//Cryptographers' Track at the RSA Conference. Springer Berlin Heidelberg, 2011: 376-392.

[9] LI J, AU M H, SUSILO W, et al. Attribute-based signature and its applications[C]//The 5th ACM Symposium on Information, Computer and Communications Security. ACM, 2010: 60-69.

[10] SU J, CAO D, ZHAO B, et al. ePASS: An expressive attribute-based signature scheme with privacy and an unforgeability guarantee for the Internet of Things[J]. Future Generation Computer Systems, 2014, 33: 11-18.

[11] LI J, CHEN X, HUANG X. New attribute–based authentication and its application in anonymous cloud access service[J]. International Journal of Web and Grid Services, 2015, 11(1): 125-141.

[12] CHASE M, CHOW S S M. Improving privacy and security in multi-authority attribute-based encryption[C]//The 16th ACM Conference on Computer and Communications Security. ACM, 2009: 121-130.

作者简介：

莫若（1990-），男，陕西渭南人，西安电子科技大学博士生，主要研究方向为密码学、信息安全等。

马建峰（1963-），男，陕西西安人，博士，西安电子科技大学教授、博士生导师，主要研究方向为网络与信息安全等。

刘西蒙（1989-），男，陕西西安人，博士，新加坡管理大学助理研究员，主要研究方向为密码学、网络安全等。

李琦（1989-），男，江苏淮安人，博士，南京邮电大学讲师，主要研究方向为密码学、信息安全等。