doi:10.11959/j.issn.1000-436x.2016263

对 2 个属性基签名方案安全性的分析和改进

杨骁[1]，向广利[1]，魏江宏[2,3]，孙瑞宗[1]

（1. 武汉理工大学计算机科学与技术学院，湖北 武汉 430070；2. 解放军信息工程大学，河南 郑州 450001；
3. 数字工程与先进计算国家重点实验室，河南 郑州 450001）

摘 要：为了克服已有属性基签名机制在安全性、效率和签名策略上的缺陷，Ma 等和 Cao 等分别提出了一个单属性机构环境下的门限属性基签名体制和多属性机构环境下签名策略支持属性的与、或、门限操作的属性基签名体制，并在计算性 Diffie-Hellman 假设下给出了相应体制的安全性证明。通过给出具体的攻击方法，指出这 2 个属性基签名方案都是不安全的，均不能抵抗伪造攻击，无法在实际中应用。此外，分析了这 2 个方案不安全的原因，并给出了针对 Ma 等方案的一种改进措施。

关键词：属性基签名；安全性分析；伪造攻击

中图分类号：TP309 **文献标识码**：A

Security analysis and improvement of two attribute-based signature schemes

YANG Xiao[1], XIANG Guang-li[1], WEI Jiang-hong[2,3], SUN Rui-zong[1]

(1. School of Computer Science and Technology, Wuhan University of Technology, Wuhan 430070, China;
2. PLA Information Engineering University, Zhengzhou 450001, China;
3. Stake Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China)

Abstract: In order to overcome the drawbacks of current attribute-based signature (ABS) schemes in terms of security, efficiency and signing policy, Ma, et al. and Cao, et al. respectively proposed a threshold ABS with single attribute authority and a multi-authority ABS with signing policy supporting AND, OR, threshold gates, and presented the security proof of their schemes under computational Diffie-Hellman assumption. Both schemes were demonstrated have security pitfalls by presenting specified attacks against them. Specifically, their schemes are all vulnerable to forgery attack. Thus, they are not feasible for practical applications. In addition, the cause of the flaws in these ABS schemes are presented, as well as an improvement of Ma et al.'s scheme.

Key words: attribute-based signature, security analysis, forgeable attack

1 引言

为克服传统公钥密码体制在分布式网络中应用时存在的缺陷，实现密文数据的细粒度访问控制问题，Sahai 等[1]在 2005 年欧密会上提出了属性基加密（ABE, attribute based encryption）的概念。ABE 机制能够支持属性的与、或、非和门限操作，表达丰富灵活的访问控制策略，在隐私保护、组密钥管理、定向广播等领域具有良好的应用前景。如同基于身份的签名体制是建立在身份基加密的基础之上，学者在 ABE 体制研究的基础上开始设计基于属性的签名（ABS, attribute based signature）体制[2~4]和签密体制[5,6]。

ABS 是一类加强了隐私保护的数字签名体制，并在近几年得到了广泛研究。在一个 ABS 体制中，每一个签名者持有一个属性集 w 和相应的由属性机构分发的属性私钥 SK_w，即签名私钥；当签名者的属性集 w 满足一个签名策略 Γ 时，签名者就能利用其签名私钥 SK_w 在策略 Γ 下对任意消息 m 进行合法签名；通过利用公钥参数和签名策略，验证者能够验证一个签名是否合法，即签名者的属性是否满足相应的签名策略。此外，为保护签名者隐私，验证

收稿日期：2016-08-31

者只能确定签名者的属性满足相应的签名策略，而不能确定是签名者的哪些属性满足该签名策略。

2008 年，Maji 等[7]首次实现了 ABS 的概念，构造了一个在一般群模型下可证安全的 ABS 体制，其签名策略支持属性的与、或和门限操作。随后，大量不同环境下支持不同签名策略的 ABS 体制相继被提出。按照 ABS 体制中的签名策略所支持的属性操作的不同，这些 ABS 体制可分为 2 类：签名策略仅支持简单的属性门限操作的 ABS 体制[7~11]和签名策略支持属性的与、或和门限操作的 ABS 体制[12~15]；按照 ABS 体制中属性机构数目的不同，这些 ABS 体制也可分为 2 类：单属性机构下的 ABS[8,10,11]和多属性机构下的 ABS[7,9,13]。此外，若干 ABS 的变体也被相继提出，如前向安全的 ABS[16]、可追踪的 ABS[17]等。最近，Ma 等[18]对文献[9]中的单属性机构下的门限 ABS 方案的安全性进行了研究，指出其不能抵抗伪造攻击，并提出了一个在标准模型下可证安全的门限 ABS 方案（Ma-ABS）。Cao 等[19]针对已有多属性机构下 ABS 体制在安全性、签名策略、效率上的不足，提出了一个多属性机构下签名策略支持属性的与、或和门限操作的 ABS 体制（Cao-ABS）。

本文分析 Ma-ABS 和 Cao-ABS 方案的安全性，指出这 2 个方案都是不安全的。首先，在 Ma-ABS 方案中，攻击者能够从签名中直接提取出属性私钥，进而能用该私钥伪造出合法签名；其次，在 Cao-ABS 方案中，一个内部用户能用自己的属性私钥推导出整个系统的属性私钥，进而能在任何签名策略下伪造出对任意消息的合法签名，此外，一个联合了内部用户的属性机构也能够推导出整个系统的属性私钥，也能在任何签名策略下伪造出对任意消息的合法签名。此外，给出了导致这 2 个方案不安全的可能原因，并对 Ma-ABS 方案进行了相应的改进。

2　预备知识

本节简要介绍本文要用到的一些基本概念，即双线性映射、拉格朗日插值、属性树。

定义 1　双线性映射。假设 G_1 和 G_2 是 2 个阶均为大素数 p 的循环群，而 g 是 G_1 的一个生成元，双线性映射 $e:G_1\times G_1\to G_2$ 为具有以下性质的映射。

1) 双线性：若 $u,v\in G_1$，且 $a,b\in\mathbb{Z}_p$，则 $e(u^a,v^b)=e(u,v)^{ab}$。

2) 非退化性：$e(g,g)\neq 1_{G_2}$。

3) 可计算性：对任意的 $u,v\in G$，存在一个有效的多项式时间算法来计算 $e(u,v)$。

定义 2　拉格朗日插值。拉格朗日系数定义为 $\Delta_{i,S}(x)=\prod_{j\in S,j\neq i}\frac{x-j}{i-j}$，其中，$i\in\mathbb{Z}_q$，$S\subseteq\mathbb{Z}_q$。则 $\mathbb{Z}_q$ 上的一个 $d-1$ 阶多项式 $p(\cdot)$ 可通过拉格朗日插值法得到

$$p(x)=\sum_{i\in S}p(i)\Delta_{i,S}(x)$$

其中，$|S|=d$。

定义 3　属性树。令 Γ 是表示了一个签名策略的属性树，其每个节点 x 代表一个门限，用其子节点和一个门限值来描述，并记 num_x 是节点 x 的子节点数目，$k_x\,(0<k_x\leqslant num_x)$是其门限值。特别地，当 $k_x=1$ 时，该门限就是一个“或门”，当 $k_x=num_x$ 时，该门限就是一个“与门”。属性树 Γ 的每一个叶子节点 x 代表一个属性，并用函数 $att(x)$ 表示，而其相应的门限值 $k_x=1$。属性树 Γ 的每一个节点的子节点进行从 1 到 num 的任意编号，并且 Γ 中所有节点的编号唯一，而函数 $index(x)$ 则返回节点 x 所对应的编号，函数 $parent(x)$ 返回节点 x 的父节点。

3　Ma-ABS 方案安全性分析

3.1　Ma-ABS 方案回顾

在 Ma-ABS 方案中，一个属性机构集中管理整个系统的属性集，并负责为用户生成相应的属性私钥。该方案由以下 4 个算法组成。

1) Setup。首先，设定 $N=\{1,2,\cdots,n+1\}$ 为系统默认属性集合，G_1 是一个阶为素数 q 的循环群，g 是其生成元，并定义双线性映射 $e:G_1\times G_1\to G_2$ 和一个抗碰撞的散列函数 $H:\{0,1\}^*\to G_1$；然后，选择 $\mathbb{Z}_q$ 中的随机数 $y,t_1,t_2,\cdots,t_{n+1}$，并对任意 $i\in N$，令 $T_i=g^{t_i},g_1=g^y$。最后，随机选取 $g_2,h\in G_1$，公布系统公钥为 $MPK=(g,g_1,g_2,T_1,T_2,\cdots,T_{n+1},h,H(\cdot))$，而系统主密钥为 $MSK=(y,t_1,t_2,\cdots,t_{n+1})$。

2) Extract(w, MSK)。该算法输入一个用户属性集 w 和系统主密钥 MSK，输出相应于 w 的私钥。首先，随机选择一个 d 次多项式 $p(x)\in\mathbb{Z}_q[x]$，并令 $p(0)=y$；然后，对任意 $i\in w$，选择随机数 $r_i\in\mathbb{Z}_q$；最后，输出用户私钥 $sk=(\{g_2^{\frac{p(i)}{t_i}}H(i)^{\frac{r_i}{t_i}},g^{r_i}\}_{i\in w})=(\{sk_{1i},sk_{2i}\}_{i\in w})$。

3) Sign(*sk*, *m*)。该算法输入用户私钥 *sk* 和一个消息 m，输出对消息 m 的签名。对任意 $i \in w$，选择随机数 $s_i \in \mathbb{Z}_p$，输出签名 $\sigma = (w, \{sk_{1i}, sk_{2i}(g_1^m h)^{s_i}, (g_1^m h)^{s_i}\}_{i \in w}) = (w, \{\sigma_{1i}, \sigma_{2i}, \sigma_{3i}\}_{i \in \omega})$。

4) Verify(*MPK*, *m*, σ)。该算法输入系统公钥 *MPK*，消息 m，以及相应的签名 $\sigma = (\omega, \{\sigma_{1i}, \sigma_{2i}, \sigma_{3i}\}_{i \in w})$，输出对签名的验证结果。选择一个属性集 w 的子集 S，使 $|S| = d$，并验证

$$\prod_{i \in S} \left(\frac{e(\sigma_{1i}, T_i) e(H(i), \sigma_{3i})}{e(H(i), \sigma_{2i})} \right)^{\Delta_{i,S}(0)} = e(g_1, g_2) \quad (1)$$

若式(1)成立，则说明签名合法，否则签名不合法。

3.2 Ma-ABS 方案安全性分析

本节通过给出 2 种具体的攻击方法，指出 Ma-ABE 方案是不安全的。在第 1 种攻击中，攻击者能从签名中提取出用户私钥，进而用该私钥伪造出合法签名。具体的攻击流程如下。

1) 给定一个用户 u，假定其属性集为 w，相应的私钥为 $sk = (\{sk_{1i}, sk_{2i}\}_{i \in w})$，并且攻击者 $\mathcal{A}$ 记录了 u 对消息 m 的一个签名 $\sigma = (w, \{\sigma_{1i}, \sigma_{2i}, \sigma_{3i}\}_{i \in w})$。

2) 由 Ma-ABS 的 Sign 算法流程可得出，对任意 $i \in w$，式(2)成立。

$$\sigma_{1i} = sk_{1i}, \ \sigma_{2i} = sk_{2i}\sigma_{3i} \quad (2)$$

因此，攻击者 $\mathcal{A}$ 可从 σ 中直接提取用户 u 的私钥

$$sk' = \left(\left\{ \sigma_{1i}, \frac{\sigma_{2i}}{\sigma_{3i}} \right\}_{i \in w} \right) = (\{sk'_{1i}, sk'_{2i}\}_{i \in w}) \quad (3)$$

3) 由式(3)可以看出，攻击者所提取的用户私钥与由属性机构为用户所分发的私钥完全相同，因此，攻击者可用所提取的私钥伪造合法签名。

在第 2 种攻击中，给定一个消息 m 的合法签名 $\sigma = (w, \{\sigma_{1i}, \sigma_{2i}, \sigma_{3i}\}_{i \in w})$，攻击者能够生成任何消息在属性集 w 下的合法签名。具体的攻击流程如下。

1) 攻击者 $\mathcal{A}$ 得到一个消息 m 的合法签名 $\sigma = (w, \{\sigma_{1i}, \sigma_{2i}, \sigma_{3i}\}_{i \in w})$ 的合法签名，即存在属性集 w 的一个子集 S（$|S| = d$），使式(4)成立。

$$\prod_{i \in S} \left(\frac{e(\sigma_{1i}, T_i) e(H(i), \sigma_{3i})}{e(H(i), \sigma_{2i})} \right)^{\Delta_{i,S}(0)} = e(g_1, g_2) \quad (4)$$

2) 对任意一个消息 m'，攻击者 $\mathcal{A}$ 生成在 m' 在属性集合 w 下的签名：$\sigma' = \sigma = (w, \{\sigma_{1i}, \sigma_{2i}, \sigma_{3i}\}_{i \in w})$。由式(1)可知，对消息 m' 的签名的验证不需要 m' 的参与，因此，σ' 始终满足式(1)，即 σ' 是消息 m' 在属性集 w 下的一个合法签名。

Ma 等中给出了 Ma-ABS 方案的安全性证明，而事实上该证明是存在缺陷的。在文献[18]的安全性证明过程中，挑战者 $\mathcal{C}$ 在接收到一个 CDH 实例 (g, g^a, g^b) 之后，令 $g_1 = g^a, g_2 = g^b$，而 $\mathcal{C}$ 不知道 a、b。最后，当攻击者 $\mathcal{A}$ 能够伪造出一个消息 m^* 的合法签名 $\sigma^* = (w^*, \{\sigma^*_{1i}, \sigma^*_{2i}, \sigma^*_{3i}\}_{i \in w^*})$ 后，挑战者 $\mathcal{C}$ 就能通过选定一个 w^* 的 d 元子集 S^*，以式(5)解决 CDH 实例

$$\prod_{i \in S^*} \left(\frac{(\sigma^*_{1i})^{u(i)+f(i)} (\sigma^*_{3i})^{(b-1)i^n + u(i)}}{(\sigma^*_{2i})^{(b-1)i^n + u(i)}} \right)^{\Delta_{i,S^*}(0)} = g^{ab} \quad (5)$$

其中，$u(i) = -i^n$，$f(i)$ 是一个 n 次多项式。由式(5)可以看出，挑战者 $\mathcal{C}$ 在计算时，需要知道 $(b-1)i^n + f(i)$ 的值，等价于 $\mathcal{C}$ 需要知道 b 的值，进而等价于 $\mathcal{C}$ 自己解决了离散对数问题，也即 $\mathcal{C}$ 不是通过 $\mathcal{A}$ 提供的伪造签名计算 g^{ab}，而是自己计算 g^{ab}。因此，文献[18]所给出的从 Ma-ABE 的安全性到 CDH 的困难性的归约是不成立的。

3.3 Ma-ABS 方案的可能改进

通过上述安全性分析可以发现，导致 Ma-ABE 方案不安全的原因有 2 个：1) 签名没有对用户属性私钥进行有效的隐藏；2) 签名验证过程中没有所签名消息的参与。本节对 Ma-ABS 方案的 Sign 算法和 Verify 算法进行稍微地修改，使其能够抵抗上述 2 种攻击。

在 Sign 算法中，将 σ_{3i} 的计算方式修改为 $\sigma_{3i} = H(i)^{s_i}$。同时，相应的 Verify 算法中的验证等式修改为

$$\prod_{i \in S} \left(\frac{e(\sigma_{1i}, T_i) e(g_1^m h, \sigma_{3i})}{e(H(i), \sigma_{2i})} \right)^{\Delta_{i,S}(0)} = e(g_1, g_2) \quad (6)$$

容易验证，对任意合法签名，式(6)均成立。同时，由于修改了 σ_{3i} 的计算方法，攻击者不再能从签名中提取出用户私钥；通过在验证等式中计算 $g_1^m h$，将签名和相应的消息进行了绑定，攻击者也不能再进行 3.2 节给出的第 2 种攻击。此外，上述修改并没有增加 Sign 算法和 Verify 算法的计算复杂度。

4 Cao-ABS 方案安全性分析

4.1 Cao-ABS 方案回顾

在 Cao-ABS 方案中，系统属性由 K 个属性机

构共同管理，每一个用户在系统中具有一个唯一的全局标识 GID(global identity)，用户私钥由一个可信中心和用户属性所在属性机构联合分发。该方案由以下 5 个算法组成。

1) Setup。首先，选择阶为素数 q 的循环群 G_1，g 为其一个生成元，并定义双线性映射 $e:G_1\times G_1\to G_2$，设定系统属性集为 $N\subset\mathbb{Z}_q$；然后，选择随机数 $\alpha\in\mathbb{Z}_q^*$，随机群元素 $g_2\in G_1$，并令 $g_1=g^\alpha$、$R=g_2^{\frac{1}{\alpha}}$，选择 2 个安全的散列函数 $H_1,H_2:\{0,1\}^*\to G_1$，一个伪随机函数 $f_s(\cdot)$，并为每一个属性机构 $k(1\leqslant k\leqslant K)$ 选择种子 s_k；最后，公布系统公钥为 $MPK=(q,G_1,G_2,e,g,g_1,g_2,Z,R,H_1,H_2)$，其中，$Z=e(g_1,g_2)$，而系统主密钥为 $MSK=\alpha$。

3) $\text{KeyGen}_{\text{private}}$。该算法由可信中心和各个属性机构协同执行。为给具有 GID 的用户 u 生成私钥，中心机构计算式为

$$y_{k,u}=f_{s_k}(u),1\leqslant k\leqslant K,\ d_{CA}=g_2^{\alpha-\sum_{k=1}^{K}y_{k,u}},$$
$$T_k=R^{\sum_{j=1,j\neq k}^{K}y_{j,u}}=g_2^{\sum_{j=1,j\neq k}^{K}\frac{y_{j,u}}{\alpha}}\tag{7}$$

然后可信中心将 d_{CA} 和 $\{T_k\}_{1\leqslant k\leqslant K}$ 分发给用户 u。在收到可信中心分发的私钥后，对任意 $1\leqslant k\leqslant K$，用户 u 向属性机构 AA_k 发送 T_k 和其由 AA_k 管理的属性集合 $w_{k,u}$。为给用户 u 生成属性私钥，AA_k 首先令 $y_{k,u}=f_{s_k}(u)$，并对任意 $i\in w_{k,u}$，选择随机数 $r_{ki}\in\mathbb{Z}_q^*$；然后，AA_k 计算式为

$$d_{ki0}=T_kR^{y_{k,u}}H_1(i)^{r_{ki}},\ d_{ki1}=g^{r_{ki}}\tag{8}$$

AA_k 将 $sk_{k,u}=\{d_{ki0},d_{ki1}\}_{i\in w_{k,u}}$ 返回给用户 u。

最后，假定任 $1\leqslant l\neq j\leqslant K$ 满足 $w_{j,u}\cap w_{l,u}=\varnothing$，$w_u=\bigcup_{k=1}^{K}w_{k,u}$，则用户 u 的属性私钥为 $sk_u=\{d_{i0}=d_{ki0},d_{i1}=d_{ki1}\}_{i\in w_{k,u}}$。

3) $\text{KeyGen}_{\text{public}}$。该算法为每一个属性树 Γ 产生一个验证公钥。首先，从根节点 r 开始，自上而下地为 Γ 中的每一个节点 x（包括叶子节点）选择一个阶为 $d_x=k_x-1$ 的多项式 p_x，其中，k_x 是门限值。特别地，对于根节点 r，令 $p_r(0)=\alpha$，再通过随机选择其他 d_r 个点来定义 p_r。而对于其他任意一个节点 x，令 $p_x(0)=p_{\text{parent}(x)}(\text{index}(x))$，再通过随机选择其他 d_x 个点来定义 p_x。最后，当所有的多项式都确定之后，生成属性树 Γ 的验证公钥 gpk，即对任意一个叶子节点 x，计算式为

$$D_x=g^{p_x(0)},h_i=H_1(i)^{p_x(0)}\tag{9}$$

其中，$i=att(x)$

4) Sign。假设用户 u 拥有属性集 $w=\bigcup_{k=1}^{K}w_{u,k}$，以及相应的私钥 (d_{CA},sk_u)。为给消息 m 在属性树 Γ 下签名，即证明 w 确实满足该属性树（$\Gamma(w)=1$），用户首先选择随机数 $s\in\mathbb{Z}_q^*$，计算式为

$$\sigma_0=H_2(m)^sd_{CA},\sigma_0'=g^s\tag{10}$$

记 w^* 为属性树 Γ 的叶子节点所对应的属性集合，对于任意 $i\in w^*$，选择随机数 $t_i\in\mathbb{Z}_q^*$，计算式为

$$\sigma_{i0}=\begin{cases}d_{i0}H_1(i)^{t_i},i\in w\cap w^*\\ H_1(i)^{t_i}\quad,i\in\dfrac{w^*}{w}\cap w^*\end{cases}\tag{11}$$

$$\sigma_{i1}=\begin{cases}d_{i1}g^{t_i},i\in w\cap w^*\\ g^{t_i}\quad,i\in\dfrac{w^*}{w}\cap w^*\end{cases}\tag{12}$$

最后，用户 u 输出消息 m 的签名 $\sigma=(\Gamma,\sigma_0,\sigma_0',\{\sigma_{i0},\sigma_{i1}\}_{i\in w^*})$。

5) Verify。在验证消息 m 的签名 $\sigma=(\Gamma,\sigma_0,\ \sigma_0',\{\sigma_{i0},\ \sigma_{i1}\}_{i\in w^*})$ 时，首先定义一个递归算法 $VerNode(\sigma,gpk,x)$，输入为签名 σ、属性树 Γ 的验证公钥 gpk 以及节点 x，输出为 G_2 中的一个群元素或者符号 $\perp$。令 $i=att(x)$，如果节点 x 是叶子节点，则

$$VerNode(\sigma,gpk,x)=\begin{cases}\dfrac{e(\sigma_{i0},D_x)}{e(\sigma_{i1},h_i)},\dfrac{e(\sigma_{i0},D_x)}{e(\sigma_{i1},h_i)}\neq 1\\ \perp\qquad,\text{其他}\end{cases}\tag{13}$$

对于非叶子定点 x，算法 $VerNode(\sigma,gpk,x)$ 按以下方式进行：对节点 x 的所有子节点 z，调用算法 $VerNode(\sigma,gpk,z)$，并将算法输出结果记为 F_z。令 S_x 为节点 x 的子节点集的任一个 k_x 元子集，并对任 $z\in S_x$ 满足 $F_z\neq\perp$。若不存在这样的 k_x 元子集，则算法 $VerNode(\sigma,gpk,x)$ 输出 $\perp$，否则，令 $i=index(z)$，$S_x'=\{index(z):z\in S_x\}$，计算式为

$$F_x=\prod_{z\in S_x}F_z^{\Delta_{i,S_x'(0)}}=e(g,g_2)^{p_x(0)\sum_{k=1}^{K}\frac{y_{k,u}}{\alpha}}\tag{14}$$

最后，对属性树 Γ 的根节点 r 调用算法

$VerNode(\sigma, gpk, r)$，得到输出结果为 F_r，然后验证式(15)是否成立。

$$\frac{e(g,\sigma_0)F_r}{e(H_2(m),\sigma_0')}=Z \tag{15}$$

若式(15)成立，则签名合法，否则签名不合法。

4.2 对 Cao-ABS 方案安全性的分析

本节通过给出 2 种具体的攻击方法，指出 Cao-ABS 方案同样是不安全的。

内部用户伪造攻击。在这种攻击中，任意一个拥有可信中心和属性机构分发私钥的内部用户能够推导出任意属性集的属性私钥，进而能够能伪造出在任意一个属性树下的对任意消息的合法签名。具体攻击过程如下。

1) 首先，具有属性集 $w=\bigcup_{k=1}^{K} w_{u,k}$ 的内部用户 u 向可信中心和属性机构申请并得到相应的私钥。

$$d_{\mathrm{CA}}=g_2^{\alpha-\sum_{k=1}^{K} y_{k,u}},\quad T_k=g_2^{\sum_{j=1,j\neq k}^{K}\frac{y_{j,u}}{\alpha}},1\leqslant k\leqslant K \tag{16}$$

2) 用户 u 计算式为

$$T=\prod_{k=1}^{K}T_k=\prod_{k=1}^{K}g_2^{\sum_{j=1,j\neq k}^{K}\frac{y_{j,u}}{\alpha}}=g_2^{\sum_{k=1}^{K}\sum_{j=1,j\neq k}^{K}\frac{y_{j,u}}{\alpha}}=g_2^{(K-1)\sum_{k=1}^{K}\frac{y_{k,u}}{\alpha}} \tag{17}$$

3) 对属于任意一个属性 AA_k 机构的任意一个属性 i，u 选择随机数 $r_{ki}\in\mathbb{Z}_q^*$，计算式为

$$d_{ki0}=T^{\frac{1}{K-1}}H_1(i)^{r_{ki}},d_{ki1}=g^{r_{ki}} \tag{18}$$

注意到 $T_kR^{y_{k,u}}=g_2^{\sum_{k=1}^{K}\frac{y_{k,u}}{\alpha}}$，因此，对比 Cao-ABS 方案中的 $\mathrm{KeyGen}_{\mathrm{private}}$ 算法可知，用户 u 所计算的属性私钥是正确的。

4) 由步骤 3)可知，用户 u 能够生成系统属性集 N 的任意一个子集的属性私钥，因此，u 也就能在任意属性树 Γ 下对任意消息 m 进行合法签名。

属性机构伪造攻击。在这种攻击中，通过与一个内部用户合谋，属性机构能在任意属性树下对任意消息进行合法签名。具体攻击过程如下。

1) 假定一个内部用户 u 持有私钥 $\{d_{\mathrm{CA}},T_k\}$，并将其发送给属性机构 AA_k。

2) 属性机构 AA_k 计算式为

$$y_{k,u}=f_{s_k}(u),\quad T^*=T_kR^{y_{k,u}}=g_2^{\sum_{k=1}^{K}\frac{y_{k,u}}{\alpha}} \tag{19}$$

3) 属性机构 AA_k 对任意用户 u^* 生成相应于任意属性集 $w=\bigcup_{j=1}^{K}w_{u^*,j}$ 的私钥为

$$d_{\mathrm{CA}}^*=d_{\mathrm{CA}}g_2^{-y}=g_2^{\alpha-(y+\sum_{k=1}^{K}y_{k,u})},\quad y\in\mathbb{Z}_q^* \tag{20}$$

$$d_{ji0}^*=T^*R^yH_1(i)^{r_{ji}}=g_2^{(y+\sum_{k=1}^{K}y_{k,u})/\alpha}H_1(i)^{r_{ji}},\quad r_{ji}\in\mathbb{Z}_q^* \tag{21}$$

$$d_{ji1}^*=g^{r_{ji}} \tag{22}$$

在上述私钥生成过程中，实际上是令 $f_{s_k}(u^*)=y_{k,u^*}$，$\sum_{k=1}^{K}y_{k,u^*}=\sum_{k=1}^{K}f_{s_k}(u^*)=y+\sum_{k=1}^{K}y_{k,u}$，容易验证所生成的私钥 $\{d_{\mathrm{CA}}^*,\{d_{i0}^*,d_{i1}^*\}_{i\in w}\}$ 是正确的。因此，属性机构 AA_k 能够在被 w 满足的任意属性树 Γ 下对任意消息 m 进行合法签名。

Cao 等[19]虽然给出了 Cao-ABS 方案的安全性证明，而上述分析表明 Cao-ABS 方案是不安全的。事实上，文献[19]中给出的安全性证明是存在缺陷的。在该证明过程中，挑战者 $\mathcal{C}$ 在接收到一个 CDH 实例 (g,g^a,g^b) 之后，令 $g_1=g^a,g_2=g^b$（$\mathcal{C}$ 不知道 a、b），然后公布系统参数 $(q,G_1,G_2,e,g,g_1,g_2,Z,R,H_1,H_2)$。按照 Cao-ABS 方案中 Setup 算法的定义，应有 $R=g_2^{\frac{1}{a}}=g^{\frac{b}{a}}$。显然，在挑战者 $\mathcal{C}$ 令 $g_1=g^a$，$g_2=g^b$ 之后，无法生成正确地系统参数 R。若 $\mathcal{C}$ 选择随机数 $r\in\mathbb{Z}_q^*$，并令 $R=g^r$，则攻击者 $\mathcal{A}$ 能通过式(23)检测出 R 不是按照 Setup 算法所生成的系统参数。

$$e(g_1,R)=\begin{cases}e(g,g_2), & R=g_2^{\frac{1}{a}}\\ R^*, & R=g^r\end{cases} \tag{23}$$

其中，R^* 是 G_2 中的一个随机群元素。这也就意味着攻击者 $\mathcal{A}$ 能够区分开 $\mathcal{C}$ 所模拟的签名方案和真实的签名方案。在这种情况下，将 Cao-ABS 方案的安全性归约到 CDH 问题的困难性也是没有意义的。

5 结束语

作为一种新的数字签名体制，ABS 在匿名认证、访问控制等领域有着广泛的应用前景，并在近几年得到了广泛的研究。最近，Ma 等[18]和 Cao 等[19]分别提出了一个不同环境下的 ABS 方案，并证明了其安全性。本文对这 2 个 ABS 方案的安全性进行了分析，通过构造具体的攻击方法来说明它们都

不能抵抗伪造攻击。此外，从安全性证明的角度分析了这 2 个方案不安全的可能原因，并给出了 Ma-ABS 方案的一种改进措施。本文的分析表明这 2 个 ABS 方案均无法满足现实应用的安全需求，因此也就无法在实际中应用。

参考文献：

[1] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]//Advances in Cryptology-Eurocrypt 2005. 2005: 457-473.

[2] OKAMOTO T, TAKASHIMA K. Efficient attribute-based signatures for non-monotone predicates in the standard model[J]. IEEE Transactions on Cloud Computing, 2014, 2(4): 409-421.

[3] CHEN X, LI J, HUANG X, et al. Secure outsourced attribute-based signatures[J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(12): 3285-3294.

[4] WEI J, HUANG X, HU X, et al. Revocable threshold attribute-based signature against signing key exposure[C]//ISPEC 2015. 2015: 316-330.

[5] WEI J, HU X, LIU W. Traceable attribute-based signcryption[J]. Security and Communication Networks, 2014, 7(12): 2302-2317.

[6] 杨晓元, 林志强, 韩益亮. 高效的模糊属性基签密方案[J]. 通信学报, 2013, 34(Z1): 8-13.
YANG X Y, LIN Z Q, HAN Y L. Efficient fuzzy attribute-based signcryption scheme[J]. Journal on Communications, 2013, 34(Z1): 8-13.

[7] MAJI H, PRABHAKARAN M, ROSULEK, M. Attribute-based signatures: achieving attribute-privacy and collusion-resistance[EB/OL]. http://eprint.i acr.org/2008/328, 2008.

[8] KUMAR S, AGRAWAL S, BALARAMAN S, et al. Attribute based signatures for bounded multi-level threshold circuits[C]//EuroPKI 2010. 2011: 141-154.

[9] LI J, AU M, SUSILO W, XIE D, et al. Attribute-based signature and its applications[C]//The 5th ACM Symposium on Information, Computer and Communications Security-ASIACCS'10. New York, 2010: 60-69.

[10] LI J, KIM K. Hidden attribute-based signatures without anonymity revocation[J]. Information Sciences, 2010, 180(9): 1681-1689.

[11] SHAHANDASHTI S, SAFAVI N. Threshold attribute-based signatures and their application to anonymous credential systems[C]//Progress in Cryptology-AFRICACRYPT 2009. 2009: 198-216.

[12] MAJI H, PRABHAKARAN M, ROSULEK M. Attribute-based signatures[C]//CT-RSA 2011. 2011: 376-392.

[13] OKAMOTO T, TAKASHIMA K. Efficient attribute-based signatures for non-monotone predicates in the standard model[C]//Public Key Cryptography-PKC 2011. 2011: 35-52.

[14] CAO D, WANG X, WANGT, SU J. An expressive attribute-based signature scheme without random oracles[C]//2011 International Conference on Computer Application and System Modeling (ICCASM 2011). 2011: 560-564.

[15] ESCALA A, HERRANZ J, MORILLO P. Revocable attribute-based signatures with adaptive security in the standard model[C]//Proceedings of the 4th International Conference on Progress in Cryptology in Africa (AFRICACRYPT'11). 2011: 224-241.

[16] WEI J, LIU W, HU X. Forward-secure threshold attribute-based signature scheme[J]. The Computer Journal, 2015, 58(10): 2492-2506.

[17] GHADAFI E. Stronger security notions for decentralized traceable attribute-based signatures and more efficient constructions[C]//CT-RSA 2015. 2015: 391-409.

[18] 马春光, 石岚, 周长利, 等. 属性基门限签名方案及其安全性研究[J]. 电子学报, 2013, 41(5): 1012-1015.
MA C G, SHI L, ZHOU C L, et al. Threshold attribute-based signature and its security[J]. Acta Electronic Sinica, 2013, 41(5): 1012-1015.

[19] CAO D, ZHAO B, WANG X, et al. Flexible multi-authority attribute-based signature schemes for expressive policy[J]. Mobile Information Systems, 2012, 8(3): 255-274.

作者简介：

杨骁（1987-），男，湖北枝江人，武汉理工大学硕士生，主要研究方向为信息安全。

向广利（1973-），男，河南信阳人，博士，武汉理工大学教授，主要研究方向为信息安全、移动计算、计算机网络等。

魏江宏（1987-），男，甘肃通渭人，博士，解放军信息工程大学讲师，主要研究方向为应用密码学、大数据安全及隐私保护、信任管理等。

孙瑞宗（1987-），男，辽宁丹东人，武汉理工大学硕士生，主要研究方向为信息安全。