doi:10.11959/j.issn.1000-436x.2015330

基于属性的抗合谋攻击可变门限环签名方案

陈桢[1,2]，张文芳[1,2]，王小敏[1]

（1. 西南交通大学 信息科学与技术学院，四川 成都 610031; 2. 西南交通大学 信息安全与国家计算网格实验室，四川 成都 610031)

摘 要：基于属性的密码体制是基于身份密码体制的泛化和发展，它将身份扩展为一系列属性的集合，具有更强的表达性，并且拥有相同属性的成员自动组成一个环，便于隐匿签名者身份。通过对现有的基于属性门限环签名方案的深入分析，发现这些方案虽然满足匿名性要求，但拥有互补属性的恶意用户可以通过合谋伪造出有效签名。为弥补上述缺陷，首先给出基于属性门限环签名的不可伪造性、不可区分性及抗合谋攻击性的形式化定义，然后给出一个基于属性的抗合谋攻击可变门限环签名方案，其安全性可归约为 CDH（computational Diffie-Hellman）困难问题。所提方案通过在用户属性密钥中引入互不相同的秘密随机因子的方法，防止合谋攻击者利用组合私钥的方式伪造签名。在随机预言机模型下，方案被证明能够抵抗适应性选择消息的存在性伪造及合谋攻击，并具有相同签名属性集用户间的不可区分性。与同类方案相比，新方案还具备更高的运算效率。

关键词：基于属性签名；可变门限；合谋攻击；匿名性；计算 Diffie-Hellman 难题

中图分类号：TP309 **文献标识码**：A

Attribute-based alterable threshold ring signature scheme with conspiracy attack immunity

CHEN Zhen[1, 2], ZHANG Wen-fang[1, 2], WANG Xiao-min[1]

(1. School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China;
2. Key Laboratory of Information Security and National Computing Grid, Southwest Jiaotong University, Chengdu 610031, China)

Abstract: Attribute-based cryptography is a generalization and development of the identity-based cryptography, which extends the identity to a set of attributes. In the attribute-based cryptosystem, different members with the same attributes can form a signature ring automatically, with the actual signer's personl idnetity easily hided. By in-depth analysis of several attribute-based threshold ring signature schemes proposed by the earlier reseachers, it is concluded that the malicious users with the complementary attributes can conspire to forge a valid signature. In order to compensate for the defect, the proposal first gives the formal definitions of the security characteristics in attribute-based threshold ring signature scheme, such as unforgeability, indistinguishability and anti-collusion attack. Then a new attribute-based alterable threshold ring signature scheme is presented, whose security is proven equivalent to the computational Diffie-Hellman problem. By introducing an random secret parameter in each user's private key, the proposal can resist the collusion attacks. It is proven that the proposal can satisfy existential unforgeability and anti-collusion against the adaptive chosen message attack in therandom oracle model, and can meet the requirement of indistinguishability among the users with the same attributes. Besides, property analysis shows that the proposal has high efficiency.

Key words: attribute-based signature; alterable threshold; collusion attack; anonymity; computational Diffie-Hellman problem

收稿日期：2015-03-30；**修回日期**：2015-10-10

基金项目：国家自然科学基金资助项目(61371098, 61003245)；中国铁路总公司科技研究开发计划基金资助项目(2014X008-A)；四川省科技厅应用基础研究基金资助项目(2015JY0182)；中央高校基本科研业务费专项基金资助项目(SWJTU11CX041)

Foundation Items: The National Natural Science Foundation of China (61371098, 61003245); The Major Project for the Science and Technology Development of China Railway Corporation (2014X008-A); The Basic Application Research Project of Sichuan Province of China (2015JY0182); The Fundamental Research Funds for the Central Universities of China (SWJTU11CX041)

1　引言

为了简化传统公钥基础设施中密钥管理复杂的问题，Shamir 等[1]于 1984 年首次提出了基于身份密码体制（IBC, identity-based cryptography）的概念。在基于身份密码体制中，用户身份信息对应一个唯一标识符，用户的私钥和密文都与用户身份密切相关，因此在基于身份的密码体制中，难以实现个人身份的隐匿。

为了应用于对匿名性要求较高的分布式环境中，2005 年，Sahai 和 Waters[2]基于秘密共享理论，第一次引进属性的概念，提出了基于模糊身份的加密方案（Fuzzy IBE, fuzzy identity-based encryption）。在基于属性的密码体制中，用户的身份被描述成一系列属性特征的集合，从而对人群进行细粒度划分。随着基于属性密码体制逐渐成为相关领域的研究热点，一系列改进的属性基加密算法被先后提出[3~7]。Goyal 等在文献[3]中给出了密钥策略的基于属性加密方案的形式化定义。利用 Goyal 提出的访问结构，在不用暴露用户身份的情况下，也可以实现加密、签名等密码学对话。

基于属性的加密系统的思想同样可以被应用至数字签名领域中，由此形成了基于属性的数字签名（ABS, attribute based signature）的概念。2006 年，Yang 等[8]提出了基于模糊身份的签名方案，如果验证者与签名者的属性集合满足门限值，验证者可以检验该签名是否为指定签名者签署的有效签名，该方案可以看作是第一个基于属性的签名方案。2007 年，Khader[9,10]先后提出了基于属性的群签名方案和具有匿名性撤销功能的基于属性的群签名方案，并且使用自底向上（bottom-up）的方法来构造访问树。在基于属性的群签名方案中，拥有一定属性数量的群成员可以代表群对消息签名，对于验证者以及群里的其他成员来说，签名者所拥有的属性特征是隐匿的，只有群管理员知道。2008 年，郭山清等借用 Khaderl 提出的基于属性群签名方案[9]的相关定义与文献[3]中构造访问控制树的概念，提出了基于属性的签名方案[11]。该方案允许签名者使用自身拥有的特定属性进行签名，但是没有提出相关的概念定义和安全模型，也缺乏方案的安全性证明。2008 年，Maji 等[12]给出了支持任意访问结构的 ABS 方案，对基于属性的签名体制概念进行详细论述，该方案能够保护签名者的属性隐私，并证明了在一般群模型（generic group model）下是安全的。

在基于属性的签名体制中，签名者的隐私问题是一个需要关注的因素，而文献[9]和文献[11]都没有考虑到签名者的隐私保护问题，在签名的同时，也暴露了签名者的部分隐私信息。为了达到隐匿用户属性的目的，一些学者将环签名的概念应用到基于属性的签名体制中。环签名最早是由 Rivest 等[13]在 2001 年提出的，签名按照一定的规则组合成环，验证者只能够检查签名的有效性，却无法确认签名者是环中的哪一位成员。与群签名[14]不同的是，环签名没有管理员，没有组织过程，具有很强的匿名性和不可伪造性。2008 年，Li 等引入额外的缺省属性集合的概念，首次提出了基于属性的门限环签名方案[15]（ABRS, attribute based ring signature），并在计算 Diffie-Hellman（CDH, computational Diffie-Hellman）问题假设下证明了该方案的安全性。但该方案只能实现(n,n)门限，具有应用局限性。随后，一系列基于属性门限环签名方案被相继提出[16,17]。Sha-handashti 等[16]于 2009 年提出了基于属性的(k,n)门限环签名方案，只有当签名者的属性集与验证者的属性集的交集达到系统门限值 k 时，验证者才能检验签名的合法性。文献[17]中，Li 等在文献[15]的基础上进行改进，只要签名者的属性集达到系统门限值 k 时，即可产生一个合法签名，从而实现了(k,n)动态门限。随后发表的文献[18~24]在算法效率和功能上不断改善。

然而，深入分析发现，上述基于属性的门限环签名方案大都无法抵抗由恶意成员发起的合谋攻击。由于用户私钥只与属性相关，攻击者可以通过组合私钥的方式伪造出他们无法独立完成的有效签名，即拥有互补属性的恶意用户通过合谋可以冒充群体中任意合法成员产生有效的环签名。为了弥补上述缺陷，本文设计了基于属性的抗合谋攻击可变门限环签名方案。该方案在签名者属性数量满足签名断言的门限值 k 时即可产生合法签名，其中 k 可根据实际应用需求在签名断言中动态改变。同时，通过引入属性公钥 T_i，并由属性授权机构选择互不相同的秘密随机因子间接作用于分发给不同用户的属性私钥中，保证签名只能由一个用户与其相对应的属性集产生，而不能由多个用户通过组合互补属性的方式共同产生。在随机预言机模型以及 CDH 问题假设下，可以证明所提方案在适应性选择消息攻击下是存在性不可伪造的，相同签名属性集用户间具备不可区分性，并且能够根本抵抗由恶意成员相互勾结导致的合谋攻击。性能分析

表明，在安全性增强的前提下，方案的运算效率较原有方案也有所提高。

2 预备知识

本节在此给出基于属性门限环签名方案中的相关定义与困难问题假设。

2.1 拉格朗日插值法

设 $f(x)$为 x 的一个 d–1 阶多项式 f 的函数，给定多项式 f 中 d 个不同点$(x_i, f(x_i))$，则通过式(1)能唯一确定任意一个 x 对应的多项式 $f(x)$

$$f(x)=\sum_{i=1}^{d} f(x_i)\left(\prod_{j=1,j\neq i}^{d}\frac{x-x_j}{x_i-x_j}\right)$$

定义式(1)中的系数为拉格朗日系数 $\Delta_{j,S}(i)$，其中，S 是这 d 个元素的集合

$$\Delta_{j,S}(i)=\prod_{\eta\in S,\eta\neq j}\frac{i-\eta}{j-\eta}$$

2.2 双线性对

定义 1 G_1、G_2 是阶为素数 p 的循环群，g 是群 G_1 的生成元。映射 $e: G_1\times G_1\to G_2$ 是一个双线性对，如果 e 满足以下性质。

1) 双线性性：对于任意的 $g_1, g_2\in G_1$ 和 $a, b\in Z$，都有 $e(g_1^a, g_2^b)=e(g_1, g_2)^{ab}$；

2) 非退化性：对于任意的 $g_1, g_2\in G_1$，存在 $e(g_1, g_2)\neq l$，l 是 G_2 中的单位元；

3) 可计算性：存在一个有效的算法，对任意的 $g_1, g_2\in G_1$，可以计算 $e(g_1, g_2)$ 的值。

2.3 困难问题假设

定义 2 计算性 Diffie-Hellman 问题给定 g^x，$g^y\in G(x, y\in Z_q^*$未知)，求解 g^{xy}。设在时间 t 内敌手 A 成功输出 g^{xy} 的概率为：$succ_G^{CDH}(A)=\Pr[A(g^x, g^y)=g^{xy}]\leqslant\varepsilon$，其中，$\varepsilon$ 是可忽略的。如果 ε 可忽略不计，则 CDH 问题是 (t,ε) 困难的。

定义 3 判定性 Diffie-Hellman 问题给定 $g^x, g^y, g^z\in G$，输出是否满足 $z=xy \bmod q$。如果在时间 t 内敌手 A 成功解决该问题的概率为：$succ_G^{DDH}(A)=\Pr[A(g^x, g^y, g^z), z=xy \bmod q]\leqslant\varepsilon$，其中，$\varepsilon$ 是可忽略的，则 DDH 问题是 (t,ε) 困难的。

3 形式化定义与安全模型

3.1 形式化定义

本节在此给出基于属性签名方案的形式化定义。基于属性的签名方案使用断言 $(\Upsilon, term)$，其中，Υ 为某些属性的集合，Φ 为 Υ 的一些子集的非空集合，且满足条件 $term$。设签名者属性集合为 ω，一个有效的签名表示签名者拥有 Φ 中某一元素(Φ 的元素为 Υ 属性集合的子集)中的所有属性，也就是说存在属性集合 $\omega'\subseteq\omega$，且满足 $\omega'\in\Phi$。本文用 $\Upsilon_{k,\omega'}()$ 表示门限断言，则签名者至少需要拥有属性集合 ω^* 的 k 个属性才能产生合法的签名。

基于属性私钥策略的签名(*KP-ABS*)方案一般由以下 4 种算法构成。

1) 初始化算法 $Setup(1^\lambda)$：由可信的属性授权机构运行的概率性随机算法，输入安全参数 1^λ，属性授权机构输出公开参数 *params* 和系统主密钥 x。

2) 密钥生成算法 $Extract(\omega)$：由可信的属性授权机构运行的概率性随机算法，输入(*params*,*x*)，用户的属性集合 ω，可信的属性授权机构输出用户产生签名的公私钥对(*TK*,*SK*)。

3) 签名算法 $Sign(\Upsilon, \omega', m)$：由签名者运行的一个概率性算法，输入系统公开参数 *params*，消息 m，签名属性集合 $\omega'(\omega'\subset\omega, \Upsilon(\omega')=1)$，以及从属性授权机构获得的公私钥对(*TK*,*SK*)，输出签名为 σ。

4) 验证算法 $Verify(\Upsilon, params, m, \sigma)$：由验证者运行一个确定性算法，输入 m、*params* 和 σ，输出 true 或者 false。如果 $\Upsilon(\omega')=1$，则 σ 是一个有效的签名，说明签名者的属性集满足断言 Υ。

3.2 安全特性

文献[15]指出基于属性的环签名必须满足以下 2 个基本安全特性：不可伪造性和不可区分性。不可伪造性是指若敌手没有属性 ω 的私钥，则无法伪造关于属性 ω 的有效签名。不可区分性（匿名性）是指给出 2 个使用同一签名断言的有效签名，在不知道系统主密钥的前提下，即使敌手知道签名者的私钥，也无法区分这 2 个签名是否由同一个签名者签署。

基于属性的门限环签名在基于属性环签名的基础上，增加了门限特性，即只要用户拥有的属性数量达到签名断言的门限值 k 时便可产生有效环签名。然而，通过对现有的基于属性门限环签名方案的深入分析，作者发现大多数方案虽然能够满足不可伪造性和不可区分性基本要求，但却无法抵抗由恶意成员相互勾结导致的合谋攻击。在基于属性的签名中，用户的身份由多个属性特征组成的集合表示，对应集合中的每个属性，都存在相应的密钥。拥有互补属性的用户通过组合各自的密钥，可以生成他们各自无法独立完成的有效签名，本文将这种攻击称为“合谋攻击”。

在具备不可伪造性和不可区分性的基础上，一个安全的基于属性的数字签名方案还应具备抗合谋攻击性。

下面给出适用于本文算法的不可伪造性和不可区分性的形式化定义。

3.2.1 不可伪造性

定义 4 一个基于属性的数字签名在适应性选择消息和断言攻击下是存在性不可伪造的，如果没有概率多项式时间的敌手以一个不可忽略的优势在以下游戏中获胜，其中敌手的优势指其获胜的概率。

1)初始化：挑战者 C 运行初始化算法，利用系统安全参数产生公共参数 *params* 和主密钥 *x*。将 *params* 发布给敌手 A，*x* 保密。A 输出挑战断言 Υ。

2) 询问阶段：敌手 A 适应性地执行以下一系列预言机询问。

①散列询问：对 A 的每条散列值的查询，算法 C 都返回相应的散列值给 A。

②私钥解析询问：A 可以根据自己的需要选择一个属性集 ω_i，向 C 询问对应用户的私钥，C 运行 $Extract(\omega)$ 算法产生公私钥对 (TK_i, SK_{ω_i})，并将 (TK_i, SK_{ω_i}) 发送给 A。

③签名询问：A 向 C 询问在属性集 ω 和断言 Υ 下关于任意消息 *m* 的签名，C 运行 $Sign(\Upsilon, \omega, m)$ 算法，生成相应的签名 σ 并返还给 A。

④验证询问：A 请求挑战者 C 验证断言 Υ 下消息 *m* 及其签名 σ，C 运行 $Verify(\Upsilon, params, m, \sigma)$ 算法，返回 true 或者 false 给 A。

3) 伪造阶段：游戏最后，A 生成一个属性集合 ω' 的消息/签名对 $(\Upsilon^*_{\omega^*}, M^*, \sigma^*)$，并且 $\omega' \in \omega^*$，$\Upsilon^*(\omega')=1$，如果满足下面的条件，则 A 在游戏中获胜。

①$Verify(\Upsilon^*, params, m, \sigma^*)$=true。

② ω' 未提交给私钥解析预言机进行询问。

③(ω', M^*)未提交给签名预言机进行询问。

3.2.2 不可区分性

定义 5 一个基于属性的数字签名在适应性选择消息和断言攻击下是不可区分的，如果没有概率多项式时间的敌手以一个不可忽略的优势在以下游戏中获胜。

1) 初始化：同定义 4 的初始化。

2) 阶段 1：同定义 4 的询问阶段。

3) 挑战：敌手 A 选择用户 u_0 (其属性集合为 ω')，要求满足 $\Upsilon^*_{\omega^*}(\omega')=1$。敌手选择 $u_1 \neq u_0$ (其属性集合为 ω')，敌手对 (u_0, ω')、(u_1, ω') 进行私钥解析询问，获得相应密钥。挑战者 C 任意选择 $b \in \{0,1\}$，运行 $Sign(\Upsilon^*_{\omega^*}, \omega', m)$ 算法，生成关于 (u_b, ω')、消息 *m*、断言 $\Upsilon^*_{\omega^*}$ 的签名 σ^*，并将 $\sigma^*, (u_0, \omega')$,(u_1, ω') 发送给 A。

4) 阶段 2：如阶段 1，敌手 A 对 $\sigma^*, (u_0, \omega'), (u_1, \omega')$ 进行询问。

5) 猜测：敌手 A 输出对 *b* 的猜测 b'。若 $b'=b$，则敌手 A 在游戏中获胜。

基于属性门限环签名在基于属性签名基础上，通过引入门限特性，只要签名者的属性满足门限值要求，即可产生合法签名。通过对现有的门限环签名方案的深入分析，发现这些方案大多无法抵抗合谋攻击，本文在此给出基于属性门限环签名方案抗合谋攻击性的形式化定义。

3.2.3 抗合谋攻击性

定义 6 一个基于属性的门限环签名在适应性选择消息和断言攻击下是抗合谋攻击的，如果没有概率多项式时间的敌手以一个不可忽略的优势在以下游戏中获胜。

1) 初始化：同定义 4 的初始化。挑战者 A 声明挑战断言为 $\Upsilon^*_{\omega^*}$。

2) 阶段 1：同定义 4 的询问阶段。

3) 挑战：敌手 A 先选择用户 u_0（属性集合为 ω_0）和用户 u_1（属性集合为 ω_1），要求满足 $\Upsilon^*_{\omega^*}(\omega_0) \neq 1$, $\Upsilon^*_{\omega^*}(\omega_1) \neq 1$。之后 A 对 (u_0, ω_0)、(u_1, ω_1) 进行私钥解析询问，获得相应密钥集 SK_0、SK_1。敌手 A 选择 $SK_0' \subseteq SK_0$、$SK_1' \subseteq SK_1$，组合成新的密钥集合 $SK' = SK_0' \cup SK_1'$，相应的属性集为 ω'，满足 $\Upsilon^*_{\omega^*}(\omega')=1$。

4) 阶段 2：如阶段 1，敌手 A 对 $\sigma^*, (u', \omega')$ 进行询问。

5) 伪造：游戏最后，A 生成一个属性集合 ω' 的消息/签名对 $(\Upsilon^*_{\omega^*}, m, \sigma^*)$，并且 $\omega' \in \omega^*, \Upsilon^*(\omega')=1$，如果同时满足下面的条件，A 在游戏中获胜，则敌手 A 在游戏中获胜。

①$Verify(\Upsilon^*, params, m, \sigma^*)$=true。

② ω' 未被提交给私钥解析预言机进行询问。

③(ω', m)未被提交给签名预言机进行询问。

文献[15]无法抵抗合谋攻击的安全性证明。

为了描述方便，假定签名断言为 $\Upsilon_{k,\omega^*}()$，待签名消息为 *m*。多项式时间的攻击者可以通过如下步

骤对 Li-Kim 的方案进行攻击。

1) 初始化：挑战者 C 运行 *Setup*(*d*)算法，得到系统参数 $params =< g, g_1, g_2, Z, d, H_1, H_2 >$ 和系统主密钥 $mk = x$。攻击者 A 得到系统参数 *params*，但无法获得系统主密钥，挑战者 C 对主密钥进行保密。

2) 询问阶段：攻击者 A 选择 2 个签名者 u_0 (属性集为 ω_0)和 u_1 (属性集为 ω_1)，满足 $\Upsilon_{k,\omega^*}(\omega_0)\neq 1$，$\Upsilon_{k,\omega^*}(\omega_1)\neq 1$，A 向挑战者 C 进行密钥解析询问，获得相应密钥分别为

$$D_{0,i} = (g_2^{q(i)}(H_1(i))^{r_i}, g^{r_i})_{i\in\omega_0}$$

$$D_{1,i} = (g_2^{q(i)}(H_1(i))^{r_i}, g^{r_i})_{i\in\omega_1}$$

3) 伪造阶段：攻击者 A 进行以下操作。

①选择属性集 $\gamma_0 \subseteq \omega_0 \cap \omega^*$ 和 $\gamma_1 \subseteq \omega_1 \cap \omega^*$，且 $\Upsilon_{k,\omega^*}(\gamma_0 \cup \gamma_1) = 1, |\gamma_0 \cup \gamma_1| = k$，记为 $\omega' = \gamma_0 \cup \gamma_1$。

②首先选择 *d*–*k* 个缺省属性子集 $\Omega' \subseteq \Omega$，之后随机选择 $r_1', r_2', \cdots, r_d', s_1, \cdots, s_d \in Z_p$ 和 *d*–1 阶多项式 $q'(x)$，其中，$q'(0) = 0$。

③对于属性 $i \in \omega' \cup \Omega'$，计算 $\sigma_{i,1} = d_{i0} H_1(i)^{r_i'} g_2^{q'(i)} H_2(m)^{s_i}$，$\sigma_{i,2} = d_{i1} g^{r_i'}$，$\sigma_{i,3} = g^{s_i}$。

④输出 $(\Upsilon_{k,\omega^*}(), m, \sigma^* = \{\sigma_{i,1}, \sigma_{i,2}, \sigma_{i,3}\}_{i\in\omega'\cup\Omega'})$。

若 A 伪造的消息及其签名 $(\Upsilon_{k,\omega^*}(), m, \sigma^*)$ 同时满足以下 3 个条件，则攻击成功。

①*Verify*(Υ^*, *params*, *m*, σ^*)=true。

② ω' 未被提交给私钥解析预言机进行询问。

③(ω', *m*)未被提交给签名预言机进行询问。

由于在询问阶段攻击者未提交 ω'和 (ω', m) 给挑战者 C 进行询问，所以条件②、③显然成立，下面验证条件①是否成立，即验证等式 $\prod_{i\in\omega'\cup\Omega'} \left(\frac{e(g,\sigma_{i,1})}{e(H_1(i),\sigma_{i,2})e(H_2(m),\sigma_{i,3})}\right)^{\Delta_{i,S}(0)} = Z$ 是否成立。

$$\begin{aligned}
\text{左边} &= \prod_{i\in\omega'\cup\Omega'} \left(\frac{e(g,\sigma_{i,1})}{e(H_1(i),\sigma_{i,2})e(H_2(m),\sigma_{i,3})}\right)^{\Delta_{i,S}(0)} \\
&= \prod_{i\in\omega'\cup\Omega'} \left(\frac{e(g, g_2^{q(i)+q'(i)} H_1(i)^{r_i+r_i'} H_2(m)^{s_i})}{e(H_1(i), g^{r_i+r_i'}) e(H_2(m), g^{s_i})}\right)^{\Delta_{i,S}(0)} \\
&= \prod_{i\in\omega'\cup\Omega'} \left(\frac{e(g, g_2^{q(i)+q'(i)}) e(g, H_1(i)^{r_i+r_i'}) e(g, H_2(m)^{s_i})}{e(H_1(i), g^{r_i+r_i'}) e(H_2(m), g^{s_i})}\right)^{\Delta_{i,S}(0)} \\
&= \prod_{i\in\omega'\cup\Omega'} e(g, g_2)^{(q(i)+q'(i))\Delta_{i,S}(0)} = e(g_2, g)^x \\
&= \text{右边}
\end{aligned}$$

经验证，攻击者的输出 $(\Upsilon_{k,\omega^*}(), m, \sigma^* = \{\sigma_{i,1}, \sigma_{i,2}, \sigma_{i,3}\}_{i\in\omega'\cup\Omega'})$ 是 Li-Kim 方案的一组有效签名。因此，合谋攻击奏效，Li-Kim 方案并不安全。同理可证，文献[16~21]的基于属性的门限环签名方案都无法抵抗此类合谋攻击。

4 抗合谋攻击的基于属性门限环签名方案

本节提出抗合谋攻击的基于属性可变门限环签名方案，通过引入属性的公钥 T_i 和用户私有参数 λ，保证签名只能由一个用户与其相对应的属性集产生，而不能由多个用户共同完成，进而能够抵抗合谋攻击。

所提 ABS 方案支持包括门限的断言 Υ_{k,ω^*}，其中，ω^* 是签名属性的集合，*k* 为门限值。$\Upsilon_{k,\omega^*}(\omega') = \begin{cases} 1, & |\omega' \cap \omega^*| \geqslant k \\ 0, & \text{其他} \end{cases}$，即当属性集 ω' 包含属性集 ω^* 中至少 *k* 个元素时，则称属性集 ω' 满足断言 Υ_{k,ω^*}。方案由初始化、密钥生成、签名、验证 4 个阶段组成。

4.1 初始化 *Setup*(*d*)

定义属性域 *U*，*U* 中的元素为属性映射的整数 (mod *q*)。设由 *d*–1 个属性（$d \in Z_q$ 为系统安全参数）构成的缺省属性集为 $\Omega = \{\Omega_1, \cdots, \Omega_{d-1}\}$，$\Omega_i \in Z_q^*$，$1 \leqslant i \leqslant d-1$。

首先，属性授权机构 AA（attribute of authority）选择一个双线性对 $e: G_1 \times G_1 \to G_2$，其中 G_1、G_2 是 2 个 *q* 阶循环群。AA 选择散列函数 $H_1, H_2: \{0,1\}^* \to G_1$。

然后，选取生成元 $g \in G_1$，元素 $g_2 \in G_1$，随机数 $x \in Z_q$，并计算 $g_1 = g^x, Z = e(g_1, g_2)$。

最终，对于任意属性 $i \in U$，选择随机数 $t_i \in Z_q^*$，计算 $T_i = g_2^{q(i)+t_i}$。

公开参数：$params =< g, g_1, g_2, e, Z, H_1, H_2, q >$。

秘密参数：$MK =< t_1, \cdots, t_{|U|}, x >$。

属性域 *U* 对应的公钥 *PK*：$PK =< T_1, \cdots, T_{|U|} >$。

4.2 密钥生成 *Extract* (ω)

属性授权机构 AA 随机选取次数为 *d*–1 的多项式 *q*(*x*)(不对外公开)。令 *q*(0)=*x*，其余 *d*–1 个系数随机选择。

给定用户 ID 及其对应的属性集合 $\omega \subset U$，产生一个新的属性集 $\bar{\omega} = \omega \cup \Omega$，为每一个用户随机选取唯一的秘密参数 $\lambda \in Z_q$，对于任意属性 $i \in \bar{\omega}$，计算

$$S_i = g_2^{-t_i} H_1(\lambda)^{q(i)}, W = H_1(\lambda)^x \tag{1}$$

拥有属性集 ω 的用户私钥为 *SK*：$SK =< W, S_1, \cdots, S_{|\bar{\omega}|} >$。

通过为每个用户选择不同的随机因子 λ 并将其作用于该用户的属性私钥 *SK* 中，可保证在签名阶段有效的签名只能由一个用户与其对应的属性集产生，而不能通过组合不同用户的互补属性集产生。

4.3 签名 *Sign*($\Upsilon_{k,\omega^*}(), \omega', m$)

声明签名断言为 $\Upsilon_{k,\omega^*}()$，签名者的属性集为 ω，选取属性子集 $\omega' = \{i_1, i_2, \cdots, i_k\} \subseteq \omega \cap \omega^*$ 对消息 m 进行签名。随机选择 $d-k$ 个缺省属性构成缺省属性子集 $\Omega' = \{i_{k+1}, i_{k+2}, \cdots, i_d\} \subseteq \Omega$。

随机选择 $r \in Z_q$，计算

$$\sigma_1 = g^{r\sum_{i\in\omega^*\cup\Omega'}\Delta_{i,S}(0)},\ \sigma_2 = Wg_2^{r\sum_{i\in\omega^*\cup\Omega'}\Delta_{i,S}(0)} \tag{2}$$

对于任一属性 $i \in \omega^* \cup \Omega'$，计算

$$\sigma_i = \{S_i(H_2(m)g_2)^r\}_{i\in\omega'\cup\Omega'} \tag{3}$$

$$\sigma_i = \{T_i^{-1}(H_2(m)g_2)^r\}_{i\in\omega^*\setminus\omega'} \tag{4}$$

最后输出对消息 m 的签名为 $\sigma = <\sigma_1, \sigma_2, \{\sigma_i\}_{i\in\omega^*\cup\Omega'}>$，将 σ 与消息 m 发送给接收方。

4.4 验证 *Verify*($\Upsilon_{k,\omega^*}(), params, m, \sigma$)

接收方验证消息 m 的签名 $\sigma = <\sigma_1, \sigma_2, \{\sigma_i\}_{i\in\omega^*\cup\Omega'}>$ 是否满足断言 $\Upsilon_{k,\omega^*}()$，判断等式

$$\frac{\prod_{i\in\omega^*\cup\Omega'} e(g, \sigma_i T_i)^{\Delta_{i,S}(0)}}{e(H_2(m), \sigma_1)e(g, \sigma_2)} = Z \tag{5}$$

是否成立，如果成立则接收消息 m 及其签名 σ，否则拒绝。

5 方案分析

5.1 正确性分析

签名验证等式成立的条件是签名者的签名属性集 ω 中存在足够多的 k 个属性，与缺省属性子集组成一个 d 个属性的集合，利用拉格朗日插值定理，可以递归地恢复出系统主密钥 x，具体推导过程如下

$$\begin{aligned}
&\frac{\prod_{i\in\omega'\cup\Omega'} e(g, \sigma_i T_i)^{\Delta_{i,S}(0)}}{e(H_2(m), \sigma_1)e(g, \sigma_2)} \\
&= \frac{\prod_{i\in\omega'\cup\Omega'} e(g, (g_2^{-t_i} H_1(\lambda)^{q(i)} (H_2(m)g_2)^r) g_2^{q(i)+t_i})^{\Delta_{i,S}(0)}}{e(H_2(m), g^{r\sum_{i\in\omega\cup\Omega'}\Delta_{i,S}(0)})} \cdot \\
&\quad \frac{\prod_{i\in\omega^*\setminus\omega'} e(g, (T_i^{-1}(H_2(m)g_2)^r)T_i)^{\Delta_{i,S}(0)}}{e(g, g_2^{r\sum_{i\in\omega^*\cup\Omega'}\Delta_{i,S}(0)} H_1(\lambda)^x)} \\
&= \frac{\prod_{i\in\omega'\cup\Omega'} e(g, H_1(\lambda)^{q(i)} g_2^{q(i)})^{\Delta_{i,S}(0)} \prod_{i\in\omega'\cup\Omega'} e(g, (H_2(m)g_2)^r))^{\Delta_{i,S}(0)}}{e(H_2(m), g^{r\sum_{i\in\omega'\cup\Omega'}\Delta_{i,S}(0)}) e(g, g_2^{r\sum_{i\in\omega'\cup\Omega'}\Delta_{i,S}(0)} H_1(\lambda)^x)}
\end{aligned}$$

$$\begin{aligned}
&= \prod_{i\in\omega'\cup\Omega'} e(g, g_2^{q(i)})^{\Delta_{i,S}(0)} \\
&= e(g, g_2)^x \\
&= Z
\end{aligned}$$

5.2 安全性分析

定理 1　在随机预言机模型及 CDH 问题假设下，本文提出基于属性的签名方案在适应性选择消息攻击下是抗存在性伪造的。

证明　假定存在一个适应性选择消息的攻击者 A 能够在多项式时间内以 ε 的优势攻破了本方案，记攻击者 A 访问 H_i(i=1,2)预言机、私钥解析预言机、签名预言机的次数分别为 $q_{\mathrm{H}i}$、q_k、q_s，则存在一个 ε' 算法 C，以 $\varepsilon' \approx \dfrac{\varepsilon}{q_{H_1} q_{H_2} \binom{d-k}{d-1}}$ 的优势解决 CDH 问题。

假定给算法 C 一个 CDH 问题的实例：给定 $g, g^x, g^y \in G_1$，C 的目标是调用 A 为子程序，最后输出 CDH 问题的一个解 g^{xy}。C 仿真如下。

1) 初始化：C 运行 *Setup*(d) 算法，令 $g_1 = g^x, g_2 = g^y$。设置安全参数 $d \in Z_q^*$，发送公开参数 $params = <g, g_1, g_2, e, Z, H_1, H_2, q>$ 给 A。A 输出挑战断言为 $\Upsilon_{k,\omega^*}(), 1 \leqslant k \leqslant d, |\omega^*| = k$。C 随机选择缺省属性集 $\Omega^* \subseteq \Omega, |\Omega^*| = d - k$。

2) H_1-询问：C 维护一个含数组 $(\omega_i, \lambda_i, Q_i)$ 的列表 H_1^{list}。C 选择随机数 $\delta \in [1, q_{H_2}]$。当 A 对 λ_i 进行 H_1 询问时，如果该询问值已在列表中，C 返回对应的 Q_i 值。否则 C 操作如下。

①如果 $\omega_i \subseteq \omega^* \cup \Omega^*$，C 选择随机数 $\beta_i \in Z_q^*$，返回 $Q_i = H_1(\lambda_i) = g^{\beta_i}$ 给 A。C 记录 $(\omega_i, \lambda_i, Q_i)$ 到列表 H_1^{list}。

②否则，C 选择随机数 $\beta_i, \gamma_i \in Z_q^*$，返回 $Q_i = H_1(\lambda_i) = g_1^{-\beta_i} g^{\gamma_i}$ 给 A。C 记录 $(\omega_i, \lambda_i, Q_i)$ 到列表 H_1^{list}。

3) H_2-询问：C 维护一个含数组 (m_i, h_i) 的列表 H_2^{list}。当 A 对 m_i 进行 H_2 询问时，如果该询问值已在列表中，C 返回对应的值 h_i，否则 C 操作如下。

①如果 $i = \delta$，C 选择随机数 $\beta_\delta \in Z_q^*$，返回 $h_\delta = H_2(m_i) = g^{\beta_\delta}$ 给 A。C 记录 (m_i, h_i) 到列表 H_2^{list}。

②否则，C 选择随机数 $\alpha_i, \beta_i' \in Z_q^*$，返回 $h_i = H_2(m_i) = g_1^{\alpha_i} g^{\beta_i'}$ 给 A。C 记录 (m_i, h_i) 到列表 H_2^{list}。

4) 密钥解析询问：C 维护一个含有数组 $(\omega_i,\lambda_i,\{T_j,S_j\}_{j\in\omega_i},Q_i)$ 的列表 key^{list}。当 A 询问具有属性集 ω_i 的用户 λ_i 的公私钥对时，C 检查列表 key^{list} 中是否有对应的询问结果。如果有，则返回对应的值 $\{T_j,S_j\}_{j\in\omega_i}$。否则，对于属性 $j\in\omega_i$，C 操作如下。

①选取缺省属性子集 $\Omega_i'\subseteq\Omega$，如果属性 $j\in(\omega_i\cap\omega^*)\cup\Omega_i'$，则令 $S_j=g_2^{-t_j}H_1(\lambda_i)^{\tau_j}$，$T_j=g_2^{\tau_j+t_j}$，其中，$\tau_j,t_j\in Z_q^*$。等价于隐式地选择一个 d–1 次多项式 $q(x)$，并且满足条件 $q(i)=\tau_j$，$q(0)=x$。C 返回结果给 A，并记录 $(\omega_i,\lambda_i,\{T_j,S_j\}_{j\in\omega_i},Q_i)$ 到列表 key^{list}。

②否则，C 停止并输出“FAILURE”（该事件用 E_1 表示）。

5) 签名询问：当 A 在断言 $\Upsilon_{k,\omega^*}()$ 下对 (ω_t,λ_i,m_i) 进行签名询问时，C 操作如下。

①如果 $|\omega^*\cap\omega_i|\geqslant k$，则 C 利用密钥解析预言机产生密钥对，并且运行 $Sign(\Upsilon_{k,\omega^*}(),\omega',m)$ 算法产生签名 $\sigma=<\sigma_1,\sigma_2,\{\sigma_i\}_{i\in\omega^*\cup\Omega'}>$ 作为对 A 的应答。

②否则，C 停止并输出“FAILURE”（该事件用 E_2 表示）。

6) 伪造签名：A 选择挑战属性集 $\bar{\omega}$ 和缺省属性集 $\overline{\Omega^*}$，输出一个消息 m^* 的签名 $\sigma^*=<\sigma_1^*,\sigma_2^*,\{\sigma_i^*\}_{i\in\omega^*\cup\Omega'}>$。如果 $\overline{\Omega^*}\neq\Omega^*$ 或 $H_2(m^*)\neq g^{\beta_\delta}$，则攻击者 A 挑战失败。否则，等式 $\dfrac{\prod_{i\in\omega^*}e(g,\sigma_iT_i)^{\Delta_{i,S}(0)}}{e(H_2(m),\sigma_1)e(g,\sigma_2)}=Z$ 成立，即 A 赢得游戏。因为 $H_1(\lambda_i)=g^{\beta_i}$，$H_2(m^*)=g^{\beta_\delta}$，则

$$\frac{\prod_{i\in\omega^*\cup\Omega'}e(g,\sigma_iT_i)^{\Delta_{i,S}(0)}}{e(H_2(m),\sigma_1)e(g,\sigma_2)}=\frac{\prod_{i\in\omega^*\cup\Omega'}e(g,(g_2^{-t_i}H_1(\lambda)^{q(i)}(H_2(m)g_2)^r)g_2^{q(i)+t_i})^{\Delta_{i,S}(0)}}{e(g,g^{\beta_\delta r\sum_{i\in\omega\cup\Omega',\Delta_{i,S}(0)}})}\cdot\frac{\prod_{i\in\omega^*\setminus\omega'}e(g,(T_i^{-1}(H_2(m)g_2)^r)T_i)^{\Delta_{i,S}(0)}}{e(g,g_2^{r\sum_{i\in\omega^*\cup\Omega'}\Delta_{i,S}(0)}H_1(\lambda)^x)}$$

$$=\frac{\prod_{i\in\omega^*\cup\Omega'}e(g,H_1(\lambda)^{q(i)}g_2^{q(i)})^{\Delta_{i,S}(0)}\prod_{i\in\omega'\setminus\omega'}e(g,(g_2H_2(m))^r))^{\Delta_{i,S}(0)}}{e(g,g^{\beta_\delta r\sum_{i\in\omega^*\cup\Omega',\Delta_{i,S}(0)}})e(g,g_2^{r\sum_{i\in\omega^*\cup\Omega',\Delta_{i,S}(0)}}H_1(\lambda)^x)}$$

$$=\prod_{i\in\omega'}e(g,g_2^{q(i)})^{\Delta_{i,S}(0)}$$

$$=e(g,g_2)^x$$

$$=e(g,g^{xy})$$

所以 C 成功地计算出 $g^{xy}=\dfrac{\prod_{i\in\omega^*}\sigma_i^*}{\sigma_1^{*\beta_\delta}\sigma_2^*}$，从而输出 $\dfrac{\prod_{i\in\omega^*}\sigma_i^*}{\sigma_1^{*\beta_\delta}\sigma_2^*}$ 作为对 CDH 问题的一个实例的解答。

下面分析 C 在这个游戏中的优势。

首先对 H_1、H_2 询问的回答和现实世界一样是不可区分的，因为每个应答在 Z_q^* 中是均匀分布的，且对 H_1、H_2 询问的应答是有效的。

对密钥解析预言机和签名预言机的回答是有效的，除非事件 E_1 或 E_2 发生。

如果 A 伪造了一个有效的签名，则 C 能解决 CDH 问题的一个实例。

总而言之，如果事件 E_1 和 E_2 都没有发生，则 C 能攻破所提方案。现在计算 C 获胜的概率：从 $d-1$ 个元素的缺省属性集 Ω 获取正确的 $d-k$ 个元素的属性子集 Ω^* 的概率为 $\dfrac{1}{\binom{d-k}{d-1}}$，$H_2(m^*)=g^{\beta_\delta}$ 正确的概率为 $\dfrac{1}{q_{H_2}}$，A 选择挑战属性 $\bar{\omega}$ 的概率至少为 $\dfrac{1}{q_{H_1}}$，所以 C 解决 CDH 问题的优势为：$\varepsilon'\approx\dfrac{\varepsilon}{q_{H_1}q_{H_2}\binom{d-k}{d-1}}$。

定理 2 在随机预言机模型及 DDH 问题假设下，本文提出基于属性的签名方案是不可区分的。

证明 假定存在一个适应性选择消息的攻击者 A 能够在多项式时间内以 ε 的优势攻破了本方案，记攻击者 A 访问 $H_i(i=1,2)$预言机、私钥解析预言机、签名预言机的次数分别为 q_{H_i}、q_k、q_s，则存在一个 ε' 算法 C，以 $\varepsilon'\approx\dfrac{\varepsilon}{q_{H_1}q_r^2\binom{d-k}{d-1}}$ 的优势解决 DDH 问题。

假定给算法 C 一个 DDH 问题的实例：给定 $g^x,g^y,g^z\in G$，C 的目标是调用 A 为子程序，判断是否满足 $z=xy\bmod q$。C 仿真如下。

1)初始化：挑战者 C 运行 *Setup*(*d*)算法，令

$g_1=g^x, g_2=g^y, g_1'=g, g_2'=g^z$。设置安全参数 $d\in Z_q^*$，发送公开参数 $params=<g,g_1,g_2,e,Z,H_1,H_2,q>$ 与系统主密钥 x，将公共参数发送给敌手 A。敌手 A 声明他将要挑战的签名断言：$\Upsilon_{k,\omega^*}(),1\leqslant k\leqslant d,|\omega^*|=k$。

2) 阶段 1：如定理 1 所示，A 可进行多项式界次数的询问，H_1 询问、H_2 询问、密钥解析询问、签名询问。

密钥解析询问：C 维护一个含有数组 $(\omega_i,\lambda_i,\{T_j,S_j\}_{j\in\omega_i},Q_i)$ 的列表 key^{list}。当 A 询问具有属性集 ω_i 的用户 λ_i 的公私钥对时，C 检查列表 key^{list} 中是否有对应的询问结果。如果有，则返回对应的值 $\{T_j,S_j\}_{j\in\omega_i}$。否则，对于属性 $j\in\omega_i$，C 操作如下。

①选取缺省属性子集 $\Omega_i'\subseteq\Omega$，如果属性 $j\in(\omega_i\cap\omega^*)\cup\Omega_i'$，则令 $S_j=g_2^{-t_j}H_1(\lambda_i)^{\tau_j}$，$T_j=g_2^{\tau_j+t_j}$，其中，$\tau_j,t_j\in Z_q^*$。等价于隐式地选择一个 d–1 次多项式 $q(x)$，并且满足条件 $q(i)=\tau_j$，$q(0)=x$。C 返回结果给 A，并记录 $(\omega_i,\lambda_i,\{T_j,S_j\}_{j\in\omega_i},Q_i)$ 到列表 key^{list}。

②否则，C 停止并输出“FAILURE”（该事件用 E_1 表示）。

签名询问：当 A 在断言 $\Upsilon_{k,\omega^*}()$ 下发送一个挑战用户 λ_i，一个随机消息 M 和一个满足签名断言的属性集合 ω_i 给挑战者 C 进行签名询问。C 操作如下。

①如果 $|\omega^*\cap\omega_i|\geqslant k$，则 C 利用密钥解析预言机产生密钥对，并且运行 $Sign(\Upsilon_{k,\omega^*}(),\omega',m)$ 算法产生签名 $\sigma=<\sigma_1,\sigma_2,\{\sigma_i\}_{i\in\omega^*\cup\Omega'}>$ 作为对 A 的应答。

②否则，C 停止并输出“FAILURE”（该事件用 E_2 表示）。

3) 挑战：敌手 A 挑战方案的不可区分性。选择用户 λ_0（属性集合为 ω_0），要求存在属性子集 $\gamma\subseteq\omega_0$，满足 $\Upsilon_{k,\omega^*}(\gamma)=1$。A 对 (λ_0,ω_0) 进行密钥解析询问，获得相应密钥对 $\{T_j,S_j\}_{j\in\omega_0}$。A 分别在 $g_1=g^x,g_2=g^y$ 或 $g_1'=g,g_2'=g^z$ 的情况下进行签名询问，C 运行 $Sign(\Upsilon_{k,\omega^*}(),\omega',m)$ 算法产生签名 $\sigma_0=<\sigma_1^0,\sigma_2^0,\{\sigma_i^0\}_{i\in\omega^*\cup\Omega'}>$、$\sigma_1=<\sigma_1^1,\sigma_2^1,\{\sigma_i^1\}_{i\in\omega^*\cup\Omega'}>$。挑战者 C 随机选择 $b\in\{0,1\}$，发送 σ_b 给 A。

4) 阶段 2：如阶段 1，A 进行多项式界次数的询问。

5) 猜测：A 输出对 b 的猜测 b' 给挑战者 C。

若 $b=b'$，则 A 赢得游戏，即 A 能够破坏本方案的不可区分性。因此，当 $z=xy \bmod q$ 时，

$$\frac{\prod_{i\in\omega^*\cup\Omega'}e(g,\sigma_i^0T_i)^{\Delta_{i,S}(0)}}{e(H_2(m),\sigma_1^0)e(g,\sigma_2^0)}=\frac{\prod_{i\in\omega^*\cup\Omega'}e(g,\sigma_i^1T_i)^{\Delta_{i,S}(0)}}{e(H_2(m),\sigma_1^1)e(g,\sigma_2^1)}$$

C 成功输出 $b\overset{?}{=}b'$ 作为对 CDH 问题的一个实例的解答。

下面分析 C 在这个游戏中的优势。

①对密钥解析预言机和签名预言机的回答是有效的，除非事件 E_1 或 E_2 发生。

②如果 A 能够区分签名与签名间的不同，则 C 能解决 DDH 问题的一个实例。

总而言之，如果事件 E_1 和 E_2 都没有发生，则 C 能攻破所提方案的不可区分性。现在计算 C 获胜的概率：从 $d-1$ 个元素的缺省属性集 Ω 获取正确的 $d-k$ 个元素的属性子集 Ω^* 的概率为 $\frac{1}{\binom{d-k}{d-1}}$，2 次选择随机数 r 相同的概率为 $\left(\frac{1}{q_r}\right)^2$，A 选择挑战属性 $\overline{\omega}$ 的概率至少为 $\frac{1}{q_{H_1}}$，所以 C 解决 CDH 问题的优势为：$\varepsilon'\approx\frac{\varepsilon}{q_{H_1}q_r^2\binom{d-k}{d-1}}$。

定理 3　在随机预言机模型及 CDH 问题假设下，本文提出的基于属性的签名方案在适应性选择消息攻击下是抗合谋攻击的。

证明　假定存在一个适应性选择消息的攻击者 A 能够在多项式时间内利用合谋攻击以 ε 的优势攻破了本方案，记攻击者 A 访问 $H_i(i=1,2)$ 预言机、私钥解析预言机、签名预言机的次数分别为 q_{Hi}、q_k、q_s，则存在一个 ε' 算法 C，以 $\varepsilon'\approx\frac{\varepsilon}{q_{H_1}q_{H_2}\binom{d-k}{d-1}}$ 的优势解决 CDH 问题。

假定给算法 C 一个 CDH 问题的实例：给定 $g,g^x,g^y\in G_1$，C 的目标是调用 A 为子程序，最后输出 CDH 问题的一个解 g^{xy}。C 仿真如下。

1) 初始化：敌手 A 声明他将要挑战的签名断言，$\Upsilon_{k,\omega^*}(),1\leqslant k\leqslant d,|\omega^*|=k$。挑战者 C 运行 $Setup(d)$ 算法，生成公共参数 $params=<g,g_1,g_2,e,Z,H_1,H_2,q>$ 与系统主密钥 x。将公共参数发送给敌手 A。

2) 阶段 1：A 可进行多项式界次数的询问：H_1

询问、H_2 询问、密钥解析询问、签名询问。

密钥解析询问：C 维护一个含有数组 $(\omega_i,\lambda_i,\{T_j,S_j\}_{j\in\omega_i},Q_i)$ 的列表 key^{list}。当 A 询问具有属性集 ω_i 的用户 λ_i 的公私钥对时，C 检查列表 key^{list} 中是否有对应的询问结果。如果有，则返回对应的值 $\{T_j,S_j\}_{j\in\omega_i}$。否则，对于属性 $j\in\omega_i$，C 操作如下。

①选取缺省属性子集 $\Omega_i^{'}\subseteq\Omega$，如果属性 $j\in(\omega_i\cap\omega^*)\cup\Omega_i^{'}$，则令 $H_1(\lambda_i)=g^{\lambda_i}$，则 $S_j=g_2^{-t_j}g^{\lambda_i\tau_j}$，$T_j=g_2^{\tau_j+t_j}$，其中，$\tau_j,t_j\in Z_q^*$。等价于隐式地选择一个 $d-1$ 次多项式 $q(x)$，并且满足条件 $q(i)=\tau_j$，$q(0)=x$。C 返回结果给 A，并记录 $(\omega_i,\lambda_i,\{T_j,S_j\}_{j\in\omega_i},Q_i)$ 到列表 key^{list}。

②否则，C 停止并输出“FAILURE”（该事件用 E_1 表示）。

签名询问：当 A 在断言 $\Upsilon_{k,\omega^*}()$ 下发送一个挑战用户 λ_i、一个随机消息 M 和一个满足签名断言的属性集合 ω_i 给挑战者 C 进行签名询问，C 操作如下。

①如果 $|\omega^*\cap\omega_i|\geqslant k$，则 C 利用密钥解析预言机产生密钥对，并且运行 $Sign(\Upsilon_{k,\omega^*}(),\omega',m)$ 算法产生签名 $\sigma=<\sigma_1,\sigma_2,\{\sigma_i\}_{i\in\omega^*\cup\Omega'}>$ 作为对 A 的应答。

②否则，C 停止并输出“FAILURE”（该事件用 E_2 表示）。

3) 挑战：敌手 A 挑战方案的抗合谋攻击性。选择用户 λ_0、λ_1（属性集合分别为 ω_0、ω_1），要求存在属性子集 $\gamma_0\subseteq\omega_0$、$\gamma_1\subseteq\omega_1$，满足 $\Upsilon_{k,\omega^*}(\gamma_0\cup\gamma_1)=1$。A 对 (λ_0,ω_0)、(λ_1,ω_1) 进行密钥解析询问，获得相应公私钥集 $(SK_{0,i}=g_2^{-t_i}g^{\lambda_0 q(i)}$，$TK_{0,i}=g_2^{q(i)+t_i}$，$W_0=g^{\lambda_0 x})_{i\in\omega_0}$、$(SK_{1,i}=g_2^{-t_i}g^{\lambda_1 q(i)},TK_{1,i}$，$W_1=g^{\lambda_1 x})_{i\in\omega_1}$。因为 $\lambda_0\neq\lambda_1$，所以 A 重新生成用户 λ_1 的密钥，选择随机数 $\gamma_i\in Z_q^*$，$(SK_{1,i}^{'}=(SK_{1,i}T_i)^{\frac{\lambda_0}{\lambda_1}}g_2^{-\gamma_i}=g_2^{-\gamma_i}g^{\lambda_0 q(i)}$，$TK_{1,i}^{'}=g_2^{\gamma_i}$，$W_1^{'}=(W_1)^{\frac{\lambda_0}{\lambda_1}}=g^{\lambda_0 x})_{i\in\omega_1}$。选择属性子集 γ_0、γ_1 组合成新的密钥集合 $(SK_k^{'}=\{SK_{0,k}\}_{k\in\gamma_0}\cup\{SK_{1,k}^{'}\}_{k\in\gamma_1}$，$TK_k^{'}=g_2^{q(k)+t_k})_{k\in\gamma_0\cup\gamma_1}$，相应的属性集为 $\omega'=\gamma_0\cup\gamma_1$，满足 $\Upsilon_{k,\omega^*}^*(\omega')=1$。

4) 阶段 2：如阶段 1，A 进行多项式界次数的询问。

5) 伪造：游戏最后，A 生成属性集合 ω' 的消息/签名对 $(\Upsilon_{\omega^*}^*,m,\sigma^*)$，并且 $\omega'\in\omega^*$，$\Upsilon_{k,\omega^*}^*(\omega')=1$，A 请求挑战者 C 验证断言 Υ_{k,ω^*}^* 下消息 m 及其签名 σ^*，C 运行 $Verify(\Upsilon_{k,\omega^*}^*,params,m,\sigma^*)$ 算法，判断等式 $\frac{\prod_{i\in\omega^*\cup\Omega'}e(g,\sigma_iT_i)^{\Delta_{i,S}(0)}}{e(H_2(m),\sigma_1)e(g,\sigma_2)}=Z$ 是否成立。若等式 $\frac{\prod_{i\in\omega^*}e(g,\sigma_iT_i)^{\Delta_{i,S}(0)}}{e(H_2(m),\sigma_1)e(g,\sigma_2)}=Z$ 成立，即 A 赢得游戏。则

$$
\begin{aligned}
&\frac{\prod_{i\in\omega^*\cup\Omega'}e(g,\sigma_iT_i)^{\Delta_{i,S}(0)}}{e(H_2(m),\sigma_1)e(g,\sigma_2)}\\
&=\frac{\prod_{i\in\gamma_1\cup\Omega_1^{'}}e(g,(g_2^{-t_i}H_1(\lambda_0)^{q(i)}(H_2(m)g_2)^r)g_2^{q(i)+t_i})^{\Delta_{i,S}(0)}}{e(H_2(m),g^{r\sum_{i\in\omega_1\cup\Omega_1^{'}}\Delta_{i,S}(0)})}\cdot\\
&\quad\frac{\prod_{i\in\gamma_1\cup\Omega_1^{'}}e(g,(g_2^{-\gamma_i}g^{\lambda_1 q(i)}(H_2(m)g_2)^r)g_2^{q(i)+\gamma_i})^{\Delta_{i,S}(0)}}{e(g,g_2^{r\sum_{i\in\omega^*\cup\Omega'}\Delta_{i,S}(0)}g^{\lambda_1 x})}\cdot\\
&\quad\frac{\prod_{i\in\omega^*\setminus\omega'}e(g,(T_i^{-1}(H_2(m)g_2)^r)T_i)^{\Delta_{i,S}(0)}}{1}\\
&=\prod_{i\in\omega^*}e(g,g_2^{q(i)})^{\Delta_{i,S}(0)}\\
&=e(g,g_2)^x\\
&=e(g,g^{xy})
\end{aligned}
$$

所以 C 成功地计算出 $g^{xy}=\frac{\prod_{i\in\omega^*}\sigma_i^*}{\sigma_1^{*\beta_\delta}\sigma_2^*}$，从而输出 $\frac{\prod_{i\in\omega^*}\sigma_i^*}{\sigma_1^{*\beta_\delta}\sigma_2^*}$ 作为对 CDH 问题的一个实例的解答。

下面分析 C 在这个游戏中的优势。

①首先对 H_1、H_2 询问的回答和现实世界一样是不可区分的，因为每个应答在 Z_q^* 中是均匀分布的，且对 H_1、H_2 询问的应答是有效的。

②对密钥解析预言机和签名预言机的回答是有效的，除非事件 E_1 或 E_2 发生。

③如果 A 利用合谋攻击伪造了一个有效的签名，则 C 能解决 CDH 问题的一个实例。

总而言之，如果事件 E_1 和 E_2 都没有发生，则 C 能攻破所提方案。现在计算 C 获胜的概率：从 $d-1$ 个元素的缺省属性集 Ω 获取正确的 $d-k$ 个元素的属性子集 Ω^* 的概率为 $\frac{1}{\binom{d-k}{d-1}}$，$H_2(m^*)=g^{\beta_\delta}$ 正确的概率为 $\frac{1}{q_{H_2}}$，A 选择挑战属性 $\bar{\omega}$ 的概率至少为 $\frac{1}{q_{H_1}}$，所以 C 解决 CDH 问题的优

势为：$\varepsilon' \approx \dfrac{\varepsilon}{q_{H_1} q_{H_2} \binom{d-k}{d-1}}$。

5.3 效率分析

本节就密钥长度、签名长度、签名阶段和验证阶段的计算代价 4 个方面与文献[15,17~21]中的方案（分别记为 LK-ABRS、Li-ABRS、W-ABRS、WQ-ABRS、T-ABRS、Fu-ABRS）进行对比，以评估本方案的性能。使用时间复杂度来评估执行方案所需的计算量，相关符号定义如下。

T_{bp}：双线性对运算所需的时间复杂度；

T_{exp}：G_1 群上的模幂运算所需的时间复杂度；

A：签名者所有属性的集合；

D：系统缺省属性集；

B：断言中声明的属性集合；

d：预定义数值；

k：断言中声明的门限值。

比较结果如表 1 所示。

在密钥长度方面，对于每一个属性 $i \in A \cup D$，文献[15,17,18,21]都以同样的方式产生 2 个密钥 (d_{i0}, d_{i1})，所以密钥长度均为 $2(|A|+d-1)|G_1|$ bit。由于本文方案引入了一个变量 W 来确保方案不受合谋攻击的威胁，所以密钥长度增加了 $1|G_1|$ bit。

对于签名长度，因为 LK-ABRS 方案采用的是 (n,n)门限，需要产生 d 个属性的签名，所以签名长度为 $3d|G_1|$ bit；W-ABRS 方案在 LK-ABRS 方案的基础上将签名长度缩短为 $2d|G_1|$ bit；而 Li-ABRS 方案、Fu-ABRS 方案与本方案采用的皆是(n,k)门限，使用上更加灵活，并且涉及到签名断言的属性集合，因此签名长度减少为$(|B|+d-k+2)|G_1|$ bit。由于 $d>B>2$，因此，本方案的签名长度小于 LK-ABRS 等方案。

在计算量方面，LK-ABRS 方案与 W-ABRS 方案需要为选择的 d 个属性集合产生签名，对应每个属性，需要进行 5 次模幂运算，所以签名计算量均为 $5dT_{\text{exp}}$。验证时，验证者同样需要对每个属性进行验证，所以验证代价为 $dT_{\text{exp}}+3dT_{\text{bp}}$。而 Li-ABRS 方案、Fu-ABRS 方案与本文方案在签名计算量和验证计算量上远远低于 LK-ABRS 和 W-ABRS 方案。相比于 Li-ABRS 方案与 Fu-ABRS 方案，本文方案验证计算量虽略有增加，但签名代价得到降低。从签名和验证总计算量来看，Li-ABRS 方案为 $(4d+2|B|-2k+2)T_{\text{exp}}+(|B|+d-k+2)T_{\text{bp}}$，Fu-ABRS 方案比 Li-ABRS 方案减少了 $1T_{\text{exp}}$，而本方案为 $(2d+2|B|-2k+3)T_{\text{exp}}+(|B|+d-k+2)T_{\text{bp}}$，比 Li-ABRS 方案减少了 $(2d-1)T_{\text{exp}}$。总体而言，本方案比 LK-ABRS、W-ABRS、Li-ABRS 和 Fu-ABRS 等方案更加高效。在列举比较的方案中，文献[19,20]中的 WQ-ABRS 和 T-ABRS 方案比较特殊，通过向量法大大减少了密钥长度和签名长度，分别减少为 $(|A|+d)|G_1|$bit 和 $3|G_1|$bit、$(|A|+d+1)|G_1|$bit 和 $2|G_1|$bit。然而，由于计算量与待签名消息 m 的比特数$|m|$成正比，因此，在签名消息较大的情况下，WQ-ABRS 和 T-ABRS 的总计算量远远高于其他方案。

上述分析表明，与现有方案相比，本方案不仅增加了抗合谋攻击特性，而且算法效率也有相应的提高。

6 结束语

本文指出文献[15~21]的基于属性的环签名方案均不能够抵抗合谋攻击，多个恶意签名者可以通过组合私钥的方式伪造出他们无法独立完成的有效签名。为了弥补上述缺陷，本文提出一个新的基于属性的可变门限环签名方案。所提方案被证明在随机预言机模型下不仅具有不可伪造性和不可区分性，而且能够根本抵抗合谋攻击。同时，性能分

表 1　　**本方案与其他方案性能比较**

方案	密钥长度/bit	签名长度/bit	签名计算量	验证计算量
LK-ABRS[15]	$2(\|A\|+d-1)\|G_1\|$	$3d\|G_1\|$	$5dT_{\text{exp}}$	$dT_{\text{exp}}+3dT_{\text{bp}}$
Li-ABRS[17]	$2(\|A\|+d-1)\|G_1\|$	$(\|B\|+d-k+2)\|G_1\|$	$(4d+2\|B\|-2k+2)T_{\text{exp}}$	$(\|B\|+d-k+2)T_{\text{bp}}$
W-ABRS[18]	$2(\|A\|+d-1)\|G_1\|$	$2d\|G_1\|$	$5dT_{\text{exp}}$	$(d+1)T_{\text{exp}}+2dT_{\text{bp}}$
WQ-ABRS[19]	$(\|A\|+d)\|G_1\|$	$3\|G_1\|$	$(k+3+\|m\|)T_{\text{exp}}$	$4T_{\text{bp}}+kT_{\text{exp}}$
T-ABRS[20]	$(\|A\|+d+1)\|G_1\|$	$2\|G_1\|$	$(k+3+\|m\|)T_{\text{exp}}$	$3T_{\text{bp}}+(\|m\|+k)T_{\text{exp}}$
Fu-ABRS[21]	$2(\|A\|+d-1)\|G_1\|$	$(\|B\|+d-k+1)\|G_1\|$	$(4d+2\|B\|-2k+1)T_{\text{exp}}$	$(\|B\|+d-k+2)T_{\text{bp}}$
本文方案	$(2\|A\|+2d-1)\|G_1\|$	$(\|B\|+d-k+2)\|G_1\|$	$(d+\|B\|-k+3)T_{\text{exp}}$	$(\|B\|+d-k+2)T_{\text{bp}}+(\|B\|+d-k)T_{\text{exp}}$

析表明新方案在签名长度、密钥长度和计算量等方面较现有方案都具有一定优势。

参考文献：

[1] SHAMIR A. Identity-based cryptosystems and signatures schemes[A]. Proc of the CRYPTO 1984[C]. Heidelberg: Springer-Verlag, 1985. 47-53.

[2] SAHAI A, WATERS B. Fuzzy identity-based encryption[A]. Proc of the Eurocrypt 2005[C]. Heidelberg: Springer-Verlag, 2005. 457-473.

[3] GOYAL V, PANDEY O, et al. Attribute-based encryption for fine-grained access control of encryption data[A]. Proc of the 13th ACM CCS[C]. New York, 2006. 89-98.

[4] ATTRAPADUNG N, IMAI H. Dual-policy attribute based encryption[A]. Proc of the ACNS'09[C]. Heidelberg: Springer-Verlag, 2009. 168-185.

[5] 李强, 冯登国, 张立武, 等. 标准模型下增强的基于属性的认证密钥协商协议[J]. 计算机学报, 2013, 36(10): 2156-2167.
LI Q, FENG D G, ZHANG L W, et al. Enhanced attribute-based authenticated key agreement protocol in the standard model[J]. Chinese Journal of Computers, 2013, 36(10): 2156-2167.

[6] 熊金波, 姚志强, 马建峰, 等. 基于属性加密的组合文档安全自毁方案[J]. 电子学报, 2014, 42(2): 366-376.
XIONG J B, YAO Z Q, MA J F, et al. A secure self-destruction scheme for composite documents with attribute based encryption[J]. Acta Electronica Sinica, 2014, 42(2): 366-376.

[7] 魏江宏, 刘文芬, 胡学先. 前向安全的密文策略基于属性加密方案[J]. 通信学报, 2014, 35(7): 38-45.
WEI J H, LIU W F, HU X X. Forward-secure ciphertext-policy attribute-based encryption scheme[J]. Journal on Communications, 2014, 35(7): 38-45.

[8] YANG P, CAO Z, Dong X. Fuzzy identity based signature with applications to biometric authentication[J]. Compute and Electrical Engineering, 2011, (37): 532-540.

[9] KHADER D. Attribute based group signatures[EB/OL]. http://eprint.iacr.org/2007/159.2007.

[10] KHADER D. Attribute based group signature with revocation[EB/OL]. http://eprint.iacr.org/2007/241.

[11] GUO S, ZENG Y. Attribute-based signature scheme[A]. Proc of the ISA 2008[C]. Busan, 2008. 509-511.

[12] MAJI H, PRABHAKARAN M, ROSULEK M. Attribute-based signatures[A]. Proc of the CT-RSA 2011[C]. Heidelberg: Springer-Verlag, 2011. 376-392.

[13] RIVEST R L, SHAMIR A, TAUMAN Y. How to leak a secret[A]. Proc of the Asiacrypt 2001[C]. Heidelberg: Springer-Verlag, 2001. 552-565.

[14] CHAUM D, HEYST E V. Group signatures[A]. Proc of the Eurocrypt 1991[C]. Heidelberg: Springer-Verlag, 1991. 257-265.

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

[16] SHAHANDASHTI S F, SAFAVI-NAINI R. Threshold attribute-based signatures and their application to anonymous credential systems[A]. Proc of the Africacrypt 2009[C]. Heidelberg: Springer-Verlag, 2009. 198-216.

[17] LI J, AU M H, SUSILO W, et al. Attribute-based signatures and its applications[A]. Proc of the 5th ACM ASIACCS[C]. 2010. 978-987.

[18] WANG W Q, CHEN S Z. An Efficient attribute-based ring signature scheme[A]. Proc of the 2009 International Forum on Computer Science-Technology and Applications[C]. 2009. 147-150.

[19] WANG W Q, CHEN S Z. Attribute-based ring signature scheme with constant-size signature[J]. IET Information Security, 2010, 4(2): 104-110.

[20] TOLUEE R, ASAAR M R, SALMASIZADEH M. Attribute-based ring signatures: security analysis and a new construction[A]. Proc of the 10th ISCISC[C]. 2013. 1-6.

[21] 付小晶, 张国印, 马春光. 一个改进的动态门限基于属性签名方案[J]. 计算机科学, 2013, 40(7): 93-97.
FU X J, ZHANG G Y, MA C G. Dynamic threshold attributes-based signature scheme[J]. Computer Science, 2013, 40(7): 93-97.

[22] 张秋璞, 徐震, 叶顶峰. 一个可追踪身份的基于属性签名方案[J]. 软件学报, 2012, 23(9): 2449-2464.
ZHANG Q P, XU Z, YE D F. Identity traceable attribute-based signature scheme[J]. Journal of Software, 2012, 23(9): 2449-2464.

[23] ESCALA A, HERRANZ J, MORILLO P. Revocable attribute-based signatures with adaptive security in the standard model[A]. Proc of the Africacrypt 2011[C]. Heidelberg: Springer-Verlag, 2011. 224-241.

[24] 陈少真, 王文强, 彭书娟. 高效的基于属性的环签名方案[J]. 计算机研究与发展, 2010, 47(12): 2075-2082.
CHEN S Z, WANG W Q, PENG S J. Efficient attribute-based ring signature schemes[J]. Journal of Computer Research and Development, 2010, 47(12): 2075-2082.

作者简介：

陈桢（1990-），男，福建福州人，西南交通大学硕士生，主要研究方向为面向云计算的签名、认证加密机制等。

张文芳[通信作者]（1978-），女，山西太原人，博士，西南交通大学副教授、硕士生导师，主要研究方向为公钥密码学、信息安全等。E-mail: wfzhang@swjtu.edu.cn。

王小敏（1974-），男，江西萍乡人，博士，西南交通大学教授、博士生导师，主要研究方向为信息安全、轨道交通安全工程等。