可否认的基于属性的指定证实人签名方案*

任 燕[1,2]，唐春明[1]
（1. 广州大学 数学与信息科学学院，广州 510006；2. 运城学院 应用数学系，山西 运城 044000）

摘 要：为了使签名人具有否认无效签名的权利，首次提出可否认的基于属性的指定证实人签名模型，构造了一个可否认的基于属性的指定证实人签名方案。在该方案中，签名者和指定的证实人均可对签名的有效性进行确认，并且可以否认无效的签名。最后，对方案的正确性进行了分析，并在随机预言模型下证明了其安全性。分析表明，本方案具有不可伪造性，并能抵抗合谋攻击。

关键词：数字签名；基于属性签名；指定证实人签名
中图分类号：TP393.04 **文献标志码**：A **文章编号**：1001-3695(2014)01-0213-04
doi:10.3969/j.issn.1001-3695.2014.01.050

Deniable attribute-based designated confirmer signature

REN Yan[1,2], TANG Chun-ming[1]
(1. *College of Mathematics & Information Science, Guangzhou University, Guangzhou* 510006, *China*; 2. *Dept. of Applied Mathematics, Yuncheng University, Yuncheng Shanxi* 044000, *China*)

Abstract: This paper proposed a new variant of designated confirmer signatures model, called deniable attribute-based designated confirmer signature, in which both the signer and the designated confirmer could run the same protocols to confirm a valid designated confirmer signatures or disavow an invalid signature. And it provided the proof of correctness and security in the random oracle (RO) model. Analysis results show that this scheme obtains the advantages of unforgeability and can resist conspiracy attack.

Key words: digital signature; attribute-based signature; designated confirmer signature

基于属性的密码体制发展了传统基于身份密码体制关于身份的概念，将身份看做是一系列属性的集合。Sahai 等人[1]第一次提出属性的概念，从此基于属性的密码体制成为研究热点之一[2~5]。基于属性的密码体制由于能通过属性将人群进行细粒度划分，所以在只知道属性而不知道对方具体身份的情况也可以方便地进行各种密码学操作及对话。

基于属性的数字签名体制的思想是由基于模糊身份签名[6]的概念发展而来，机制更为灵活，签名者可以声称签名对应于一组特定的属性或某种特定访问结构，验证者可以检验签名确实是由相应的属性或访问结构拥有者的签名[7~9]。

不可否认签名的概念是由 Chaum[10] 于 1991 年首次提出。在这种签名方案中，验证签名必须有签名者的合作，以保证签名的接收者无法滥用签名，从而保护签名者的利益。然而，该方案的一个问题是：若签名者无法合作验证签名，那么签名的接收者将无法验证签名。为了克服这个缺陷，1995 年 Chaum[11] 又提出指定证实人签名。在指定证实人签名方案中，签名者指定某一确认者对签名进行确认，如果签名者无法验证签名，指定证实人也能对签名的有效性进行确认。随后，Okamoto[12] 提出了更加有效的指定证实人签名；但是 Michels 等人[13] 指出 Okamoto 方案中的一个缺点并给出了修正方案。随后 Gentry 等人[14~19] 提出了一些指定证实人签名方案，但是这些方案要么不安全，要么效率低。2004 年 Libert 等人[20] 利用双线性对构造了基于身份的不可否认签名。

在现有的指定证实人签名方案中有一个缺点：签名者没有权利否认无效的指定确认者签名。2003 年 Galbraith 等人[21] 首次指出指定证实人签名应该允许签名者有否认无效签名的能力，但是他们没有给出更进一步的研究。Wang 等人[22] 给出了一个签名者具有否认能力的指定证实人签名正式的安全模型，同时利用双线性映射构建了一个具体的方案，克服了这个缺陷。

本文结合基于属性的签名首次构建了一个基于属性的可否认的指定证实人签名方案，在该方案中，签名者和指定的证实人均可对签名的有效性进行确认，并且可以否认无效的签名。

1 预备知识

1.1 双线性映射

设 G_1、G_2 是两个循环乘法群，G_1、G_2 的阶均为素数 q。设 $e:G_1\times G_1\to G_2$ 为一个双线性映射。假定在 G_1、G_2 上的离散对数问题(DLP 问题)都是困难的，则双线性映射满足以下性质。

1)双线性性 对任意的所有的 $P,Q\in G_1$ 和所有的 $a,b\in Z_q$ 有 $e(aP,bQ)=e(P,Q)^{ab}$。

2)非退化性 存在 $P,Q\in G_1$ 使得 $e(P,Q)\neq 1$。

3)可计算性 对于 $P,Q\in G_1$ 存在一个高效的算法计算 $e(P,Q)$。

收稿日期：2013-03-09；**修回日期**：2013-04-27 **基金项目**：国家自然科学基金资助项目(11271003,11241005)；广东省自然科学基金面上项目(S2012010009950)；广东省教育厅高层次项目(广州市教育局 2012A004)；运城学院生物数学重点实验室开放课题(SWSX201306)

作者简介：任燕(1982-)，女，山西运城人，博士研究生，主要研究方向为密码学(renyan-2000@163.com)；唐春明(1972-)，男，广东广州人，教授，博导，主要研究方向为云计算及信息安全.

1.2 拉格朗日插值定理

设 $f(x)$ 为 x 的一个次数为 n 的多项式 f 的函数，如果给定多项式 $n+1$ 个不同点 $(x_i, f(x_i))$，则通过下式能唯一确定任意一个 x 所对应的多项式 $f(x)$ 值为

$$f(x)=\sum_{i=1}^{n} f(x_i)\left(\prod_{1\leqslant k\neq i\leqslant n}(x-x_k)/x_j-x_k\right)$$

对于上式中可以定义拉格朗日系数 $\Delta_{i,s}$，其中 $i\in Z_p$，集合 s 中的元素取自 Z_p

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

1.3 本方案依赖以下困难性问题

1）离散对数问题（DLP） 给定 $P,Q\in G_1$，求 $n\in Z_q$，使得 $P=nQ$。

2）双线性对求逆问题 已知 $a=e(P,Q)$，给定 $P\in G_1$，求 $Q\in G_1$。

3）计算 Diffie-Hellman 问题（CDHP） 对 $a,b\in Z_q$，给定 (P,aP,bP)，计算 abP。

4）计算性、双线性 Diffie-Hellman（CBDH）问题 假设群 G,G_T,G 中的生成元为 g，$e:G\times G\rightarrow G_T$ 是一个双线性映射，则 $[G,G_T,e]$ 中的 CBDH 问题定义如下：

给定 (g^a,g^b,g^c,g)（其中，随机元素 $a,b,c\in Z_q^*$，计算 $e(g,g)^{abc}$。

2 可否认的基于属性的指定证实人签名方案的安全模型

定义 1 一个正确的可否认的基于属性的指定证实人签名方案包括签名者、指定证实人和验证者。由以下八部分组成：

a）系统初始化。由系统运行的一个概率性算法。输入为系统安全参数，输出系统主密钥集合和公开的参数。

b）密钥生成。输入为系统的主密钥和用户的属性集合，输出为每个属性对应的属性密钥。

c）签名。输入为系统参数，签名者的属性集合，签名者的私钥和消息 m，输出为签名者对消息 m 的签名 σ。

d）验证。输入为系统参数，签名者的公钥，消息 m 和对消息的签名，输出为比特值 b，其中 $b=1$ 表示签名有效，$b=0$ 表示签名无效。

e）指定证实人签名。输入为消息 m，签名者的私钥和确认者的公钥，输出为对消息 m 的指定确认者签名 σ'。

f）抽取。输入为消息 m，指定确认者签名 σ'，签名者的公钥，确认者的私钥和确认者的公钥，输出为对消息 m 的签名 σ。

g）确认。确认过程是一个交互协议，签名者和证实人都可以利用自己的私钥与验证者运行确认协议来确定指定证实人签名是可抽取的。

h）否认。否认过程也是一个交互协议，签名者和证实人都可以利用自己的私钥与验证者运行确认协议来确定指定证实人签名是不可抽取的。

一个可否认的基于属性的指定证实人签名方案要满足不可伪造性，并能抵抗合谋攻击。不可伪造性的定义依赖于下面的游戏。该游戏包括一个挑战者和一个敌手。

a）挑战者选择一个安全参数，运行 setup，生成主密钥和公共参数，挑战者保存密钥，将公共参数发送给敌手。

b）敌手进行多项式次的密钥生成查询、签名查询、指定证实人查询确认查询和否认查询。

c）敌手输出指定证实人签名。

若敌手输出的签名在抽后满足验证算法则称敌手赢得游戏。

定义 2 不可伪造性 一个概率多项时间的伪造算法 F 如果在运行至多 t 次，也至多进行了多项式次查询后，赢得上述游戏的概率可以忽略，则一个可否认的基于属性的指定确认者签名方案是不可伪造的。

抵抗合谋攻击基于如下的游戏，该游戏包括一个挑战者和多个敌手。

a）挑战者选择一个安全参数，运行 setup，生成主密钥和公共参数，挑战者保存密钥，将公共参数发送给每个敌手。

b）每个敌手进行多项式次的密钥生成查询，然后将所得密钥联合。

c）每个敌手都进行签名查询、指定证实人查询确认查询和否认查询。

d）敌手输出指定证实人签名。

若敌手输出的签名在抽后满足验证算法则称敌手赢得游戏。

定义 3 可以抵抗合谋攻击 多个概率多项时间的伪造算法 F 如果在运行至多 t 次，也至多进行了多项式次查询后，赢得上述游戏的概率可以忽略，则一个可否认的基于属性的指定证实人签名方案是可以抵抗合谋攻击的。

定义 4 安全性 若一个可否认的基于属性的指定证实人签名满足不可伪造性并能抵抗合谋攻击，则称该方案是安全的。

3 方案的构造

首先令 G_1 是一个阶为素数 p 的双线性群，g 是 G_1 的生成元。令 G_2 是一个阶为素数 q 的双线性群，g_2 是 G_2 的生成元。令 $e_1:G_1\times G_1\rightarrow G_2$，$e_2:G_2\times G_2\rightarrow G_3$ 代表两个双线性映射。其中，$g_2=e_1(g,g)$。群的大小由一个安全性参数 k 来确定。同时，对于 Z_p 上的元素组成的集合 S 以及 $i\in Z_p$，定义拉格朗日差值 $\Delta_{i,s}(x)$ 为

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

所有的属性均取自一个总的集合 u，大小为 $|u|$，每个属性均对应着 Z_p^* 上的一个唯一整数。

1）参数生成 输入一个安全性参数 k，首先私钥生成机构 PKG 定义所有属性的集合 u，为了简化方案，选择 Z_p^* 上的前 $|u|$ 个元素来构成集合 u，分别为 $1,2,\cdots,|u|(\mathrm{mod}\ p)$。然后，从 Z_p^* 上随机选择一系列的数：$s,t,t_1,\cdots,t_{|u|}$ 作为主密钥，定义为

$$T_t=e_1(g,g)^t,T_{t-1}=e_1(g,g)^{t-1},T_s=e_1(g,g)^s,T_s{}^{-1}=e_1(g,g)^{s-1}$$

$$T_{st-1}=e_1(g,g)^{st-1},T_{s-1t-1}=e_1(g,g)^{t-1s-1}$$

$$T_1=g^{t1},\cdots,T_{|u|}=g^{t|u|}$$

定义一个哈希函数：$H:\{0,1\}^*\rightarrow Z_q^*$，这样主密钥包含：$s,t,t_1,\cdots,t_{|u|}$ 公开参数包括 $T_t,T_{t-1},T_s,T_{s-1},T_{st-1},T_{s-1}t^{-1},T_1,\cdots,T_{|u|},G_1,G_2,G_3,e_1,e_2,H$。

2）公私钥提取 首先生成签名者 S 的公私钥。令签名者 S 的属性集合为 $\omega_1\subseteq u$，PKG 首先选择一个 $d-1$ 阶的多项式 $q(x)$，满足 $q(0)=y_1$，则每个属性对应的私钥 $D_{iS}=g^{\frac{q(i)}{t_i}}(i\in\omega_1)$，同时公开参数集 $\{E_{iS}=T_i^{st-1}\}_{i\in\omega_1}$，并把 y_1 秘密发送给 S。最后签名者 S 计算自己的私钥：

$$S_S=\prod_{i\in\omega_1}(e_1(D_{iS},E_{iS}))^{\Delta_{i,\omega_1}(0)}=e_1(g,g)^{st-1y_1}$$

公钥为:$Y_S = e_1(g,g)^{y_1 t^{-1}} = g_2^{y_1 t^{-1}}$ 及 $T_S = e_1(g,g)^{y_1}$。

同样地,对于证实人 C 的属性集合 $\omega_2 \subseteq u$,PKG 首先选择一个 $d-1$ 阶的多项式 $q'(x)$,满足 $q'(0) = y_2$,则每个属性对应的私钥 $D_{i_C} = g^{\frac{q'(i)}{t_i}}(i \in \omega_2)$,同时公开参数集合 $\{E_{i_C} = T_i^{st}\}_{i \in \omega_2}$,并把 y_2 秘密发送给证实人 C。最后证实人计算自己的私钥:

$$S_C = \prod_{i \in \omega_2} (e_1(D_{i_C}, E_{i_C}))^{\Delta_{i,\omega_2}(0)} = e_1(g,g)^{st^{-1}y_2}$$

公钥为:$Y_C = e_1(g,g)^{y_2 t^{-1}} = g_2^{y_2 t^{-1}}$ 及 $T_C = e_1(g,g)^{y_2}$。

3)签名生成　对于给定的一个消息 m,S 完成对 m 的基本签名 $\sigma = S_S^{y_1 + h}$,此处的 $h = H(m)$。

4)签名验证　收到签名 σ 后,验证等式 $e_2(\sigma, T_{s-1t-1}) = e_2(Y_S^2, g_2) e_2(Y_S, T_{t-1})^h$ 是否成立。

5)指定证实人签名　在生成一个基本签名后,签名者 S 随机选择一个 $r \in Z_q^*$,计算 $\sigma_1 = T_{t-1}^{\ r}$,$\sigma_2 = \sigma Y_C^r$,关于 m 的指定证实人签名为 $\sigma' = (\sigma_1, \sigma_2)$。

6)抽取过程　给定消息 m 和指定确认者签名 $\sigma' = (\sigma_1, \sigma_2)$,证实人可以抽取基本签名

$$\sigma = \frac{\sigma_2 S_c}{(\sigma_1 T_{st-1})^{y_2}}$$

7)确认过程　给定(m, σ', Y_S, Y_C),证实人 C 可以通过证明 $\log_{e_2(T_{s-1}, \sigma_1)} R = \log_{e_1(g,g)} T_C$ 成立,签名人可以通过证明等式 $\log_{e_2(T_{s-1}, Y_C)} R = \log_{T_{t-1}} \sigma_1$ 成立来确认签名,其中 $R = \frac{e_2(\sigma_2, T_{s-1})}{e_2(Y_S, T_S) e_2(Y_S, g_2^h)}$。则无论是证实人还是签名者可以与验证者施行如下的交互零知识协议

$$PK\{(r \vee y_2): [\log_{e_2(T_{s-1}, \sigma_1)} R = \log_{e_1(g,g)} T_C \wedge T_C = e_1(g,g)^{y_2}] \vee [\log_{e_2(T_{s-1}, Y_C)} R = \log_{T_{t-1}} \sigma_1 \wedge \sigma_1 = T_{t-1}^{\ r}]\}$$

其中　$R = \frac{e_2(\sigma_2, T_{s-1})}{e_2(Y_S, T_S) e_2(Y_S, g_2^h)}$。

8)否定过程　给定 (m, σ', Y_S, Y_C),当 $\log_{e_2(T_{s-1}, \sigma_1)} R \neq \log_{e_1(g,g)} T_C$ 且 $\log_{e_2(T_{s-1}, Y_C)} R = \log_{T_{t-1}} \sigma_1$,则说明 σ' 是对消息 m 的无效签名。从而无论是证实人还是签名者可以与验证者施行如下的交互零知识协议

$$PK\{(r \vee y_2): [\log_{e_2(T_{s-1}, \sigma_1)} R \neq \log_{e_1(g,g)} T_C \wedge T_C = e_1(g,g)^{y_2}] \vee [\log_{e_2(T_{s-1}, Y_C)} R \neq \log_{T_{t-1}} \sigma_1 \wedge \sigma_1 = T_{t-1}^{\ r}]\}$$

其中　$R = \frac{e_2(\sigma_2, T_{s-1})}{e_2(Y_S, T_S) e_2(Y_S, g_2^h)}$。

4　正确性和安全性分析

4.1　正确性分析

4.1.1　验证的正确性

验证等式 $e_2(\sigma, T_{s-1t-1}) = e_2(Y_S^2, g_2) e_2(Y_S, T_{t-1})^h$ 是成立的

证明

$$e_2(\sigma, T_{s-1t-1}) = e_2(g_2^{st^{-1}y_1(y_1+h)}, g_2^{s-1t-1}) = e_2(g_2^{t^{-1}y_1}, g_2^{t^{-1}y_1}) e_2(g_2^{t^{-1}y_1 h}, g_2^{t^{-1}}) = e_2(Y_S^2, g_2) e_2(Y_S, T_{t-1})^h$$

4.1.2　抽取的正确性

可以通过如下的过程验证抽取过程的正确性

$$\frac{\sigma_2 S_c}{(\sigma_1 T_{st-1})^{y_2}} = \frac{\sigma Y_C^r g_2^{st^{-1}y_2}}{(T_{t-1}^{\ r} g_2^{st^{-1}})^{y_2}} = \frac{\sigma g_2^{y_2 t^{-1} r} g_2^{st^{-1}y_2}}{(g_2^{t^{-1}r} g_2^{st^{-1}})^{y_2}} = \sigma$$

4.1.3　确认的正确性

对于证实人 C

$$R = \frac{e_2(\sigma_2, T_{s-1})}{e_2(Y_S, T_S) e_2(Y_S, g_2^h)} = \frac{e_2(g_2^{st^{-1}y_1^2}, g_2^{s-1}) e_2(g_2^{st^{-1}y_1 h}, g_2^{s-1}) e_2(g_2^{t^{-1}y_2 r}, g_2^{s-1})}{e_2(g_2^{t^{-1}y_1}, g_2^{y_1}) e_2(g_2^{t^{-1}y_1}, g_2^h)} = e_2(g_2^{t^{-1}y_2 r}, g_2^{s-1}) e_2(T_{s-1}, \sigma_1)^{y_2} = e_2(g_2^{s-1}, g_2^{t^{-1}r})^{y_2} = e_2(g_2^{y_2 t^{-1} r}, g_2^{s-1}) = R$$

同时 $T_C = e_1(g,g)^{y_2}$,所以 $\log_{e_2(T_{s-1}, \sigma_1)} R = \log_{e_1(g,g)} T_C$。同理可验证 $\log_{e_2(T_{s-1}, Y_C)} R = \log_{T_{t-1}} \sigma_1$。

4.2　安全性分析

定理 1　本方案不可伪造。

证明　对于一个签名,如果一个个体不满足签名者声明的属性结构,无法伪造出此签名。在本文方案,如果攻击者以不可忽略的概率伪造签名,就说明攻击者能以不可忽略的概率来解决 CBDH 难题,从而此方案是抗伪造的。假设存在一个敌手 A 能够伪造一个合法的可否认的基于属性的指定证实人签名,则能够构造一个模拟者 B,利用 A 来解决一个 CBDH 问题。模拟者 B 的算法可以根据(g^a, g^b, g^c, g)在不知道 a、b、c 的情况下,计算出 g^{abc}。

令 $P_{\text{pub}} = g_2^c$,$Y_S = g_2^a$,$T_S = g_2^b$,$Y_C = g_2^{a'}$。

1)模拟公钥查询　当敌手 A 提交属性集合 ω_i 向 B 查询所对应的公钥时,B 首先在其维护的一张(ω_i, Y_i) 列表 Y^{list} 中查找对应的 ω_i 项,如果查找不到,则利用如下规则进行答复:

$$Y_i = \begin{cases} g_2^{\ a} & w_i \cap w_1 \geqslant d \\ g_2^{\ a} & w_i \cap w_2 \geqslant d \\ g_2^{t_i} & \text{其他}(t_i \in Z_q^*) \end{cases}$$

然后把(ω_i, Y_i, t_i)存入到 Y^{list}列表,把 Y_i 返回给 A 。

2)模拟密钥提取查询　当敌手 A 提交 ω_i 向 B 查询对应私钥时,B 首先在维护列表 Y^{list}中查找 ω_i 的对应项(ω_i, Y_i, t_i),如果 $t_i \neq a$ 或者 b, 则 B 返回 $S_i = (g_2^{t_i})^c$ 和 y_i 作为 Y_i 对应的私钥,并把$(\omega_i, Y_i, S_i, y_i)$存入 E^{list}列表,否则, B 终止游戏。

3)模拟 H 查询

当敌手输入消息 m_i 之后,B 选择一个随机数 $h_i \in Z_q^*$,然后返回给 A,并把(m, h_i)存入自己维护的列表 H^{list}中。

4)模拟签名查询

敌手输入一个消息 m,签名者属性 ω_i 之后,B 首先从列表 H^{list}查找 m 的对应项,如果 m 有对应项且 $|\omega_i \cap \omega_1| < d$ 时,则 B 在其维护的 E^{list} 列表中找到$(\omega_i, Y_i, S_i, y_i)$,则计算 $\sigma^* = S_i^{y_i h_i}$。如果 m 没有对应的项且 $|\omega_i \cap \omega_1| < d$ 时,B 随机选择 $h_i \in Z_q^*$,然后计算 $\sigma^* = S_i^{y_i + h_i}$,最后把签名 σ^* 返回给敌手 A,否则,B 停止模拟。

5)模拟验证查询　敌手输入一个消息 m 的签名 σ^*,B 利用签名的验证算法来验证签名是否有效。

6)模拟指定证实人签名查询　在得到基本签名 σ^* 后,敌手输入指定证实人属性 ω_j,如果 $|\omega_j \cap \omega_2| < d$,则 B 在其维护的 E^{list}列表中找到$(\omega_j, Y_j, S_j, y_j)$后,$B$ 随机选择一个 $r^* \in Z_q^*$,计算 $\sigma_1^* = T_t^r$,$\sigma_2^* = \sigma^* Y_j^r$,则关于 m 的指定证实人签名为 $\sigma'^* = (\sigma_1^*, \sigma_2^*)$。

7)模拟抽取查询　敌手输入消息 m 和指定证实人签名

$\sigma'^{*}=(\sigma_1^{*},\sigma_2^{*})$,$B$ 可以抽取基本签名 $\sigma^{*}=\dfrac{\sigma_2^{*}S_j}{(\sigma_1^{*}T_{st-1})^{y_j}}$。

8)模拟确认、否认查询 模拟者 B 可以直接运行零知识证明协议来检验签名是否有效,或者否认无效的签名。最后,敌手 A 输出一个伪造的消息的合法签名,对应的签名者属性为 ω_i,指定证实人的属性为 ω_j。如果 $|\omega_i\cap\omega_1|<d$,$|\omega_j\cap\omega_2|<d$,则失败,退出游戏;否则,B 在列表 H^{list} 中找到 (m,h_i),然后重新与 A 进行同样的游戏,并根据分叉引理以相同的参数和选择不同的哈希函数 $H(.)$ 进行重放。则知道 B 可以获得 m 另一个基本签名 $\sigma^{**}=S_i^{y+jh_j}$ 和另一个指定证实人签名 $\sigma'^{**}=(\sigma_1^{**},\sigma_2^{**})$,满足 $h_i\neq h_j$,因为

$$\sigma^{*}=S_i^{y_i+h_i},\sigma^{**}=S_i^{y_i+h_j}$$

可以计算出

$$\frac{\sigma^{*}}{\sigma^{**}}=S_i^{y_i+h_i-y_i-h_j}=S_S^{h_i-h_j}$$

令 $h=(h_i-h_j)^{-1}(\bmod q)$,则 B 输出 $(\dfrac{\sigma^{*}}{\sigma^{**}})^{h}$ 作为 CBDH 问题的解,因为:$(\dfrac{\sigma^{*}}{\sigma^{**}})^{h}=S_S^{b}=((g_2^{a})^{c})^{b}=g_2^{abc}$。

定理 2 本方案可以抵抗合谋攻击。

证明 假设所指定的属性集合为 ω,用户 A 具有属性集合 ω_1,B 具有属性集合 ω_2,满足 $\omega_1\cup\omega_2=\omega$。但是,每个用户的属性私钥都对应着一个不同的随机多项式 $q(x)$。ω 中每个属性对应的私钥 $D_i=g^{\frac{q(i)}{t_i}}(i\in\omega)$,$\omega_1$ 每个属性对应的私钥 $D_{i_1}=g^{\frac{q_1(i)}{t_i}}(i\in\omega_1)$,$\omega_2$ 每个属性对应的私钥 $D_{i_2}=g^{\frac{q_2(i)}{t_i}}(i\in\omega_2)$。

所以即使用户的属性集合合并能够组合出符合要求的属性集合,但是它们的密钥联合起来也不能成功伪造签名。

5 结束语

结合基于属性的签名方案首次构建了一个可否认的基于属性的指定证实人签名方案。在该方案中,签名者和指定的证实人均可对签名的有效性进行确认,并且可以否认无效的签名。同时,对方案的正确性和安全性进行了分析,并证明了本方案具有不可伪造性,并能抵抗合谋攻击。

参考文献:

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

[2] BETHENCOURT J,SAHAI A,WATERS B. Ciphertext-policy attribute-based encryption[C]//Proc of the 28th IEEE Symposium on Security and Privacy. 2007: 321-334.

[3] CHEUNG L, NEWPORT C. Provably secure ciphertext policy ABE [C]//Proc of the 14th ACM Conference on Computer and Communications Security. New York: ACM Press, 2007: 456-465.

[4] PIRRETTI M,TRAYNOR P,McDANIEL P,*et al*. Secure attribute-based systems[C]//Proc of the 13th ACM Conference on Computer and Communications Security. 2006: 99-112.

[5] OSTROVSKY R, SAHAI A, WATERS B. Attribute-based encryption with nonmonotonic access structures[C]//Proc of the 14th ACM Conference on Computer and Communications Security. NewYork: ACM Press, 2007: 195-203.

[6] YANG Pi-yi,CAO Zhen-fu,DONG Xiao-lei. Fuzzy identity based signature,Report 2008 /002[R]. Shanghai:Shanghai Jiao Tong Universing,2007.

[7] LI Jin, AU Man-ho, SUSILO W, *et al*. Attribute-based signature and its applications[C]//Proc of the 5th ACM Symposium on Information, Computer and Communications Security. New York:ACM Press, 2010: 60-69.

[8] ESCALA A, HERRANZ J, MORILLO P. Revocable attribute-based signatures with adaptive security in the standard model[C]//Proc of the 4th International Conference on Progress in Cryptology-Africacrypt. Berlin:Springer-Verlag , 2011: 224-241.

[9] OKAMOTO T, TAKASHIMA K. Efficient attribute-based signatures for nonmonotone predicates in the standard model[C]//Proc of the 14th International Confernce on Practice and Theory in Public Key Cryptography Conference on Public Key Cryptography. Berlin:Springer-Verlag,2011: 35-52.

[10] CHAUM D. Zero-knowledge undeniable signature[C]// Proc of Eurocrypto. Berlin:Springer-Verlag, 1991:458-464.

[11] CHAUM D. Designated confirmer signatures[C]// Proc of Eurocrypto. Berlin:Springer-Verlag, 1995: 86-91.

[12] OKAMOTO T. Designated confirmer signatures and public-key encryption are equivalent[C]// Proc of Cryptology'94. Berlin:Springer-Verlag, 1994:61-74.

[13] MICHELS M, STADIER M. Generic constructions for secure and efficient confirmer signature schemes[C]//Proc of Advances in Cryptology-EUROCRYPT. Berlin:Springer,1998: 406-421.

[14] GENTRY C, MOLNAR D, RAMZAN Z. Efficient designated confirmer signatures without random oracles or general zero-knowledge proofs[C]//Proc of Advances in Cryptology-ASIACRYPT. Berlin: Springer, 2005: 662-681.

[15] GOIDWASSER S, WAISBARD E. Transformation of digital signature schemes into designated confirmer signature schemes[C]//LNCS,vol 2951. Berlin :Springer, 2004: 77-100.

[16] MICHELS M, STADLER M. Generic constructions for secure and efficient confirmer signature schemes[C]// Proc of Eurocrypt. 1998: 458-464.

[17] OKAMOTO T. Designated confirmer signatures and public-key encryption are equivalent[C]// Proc of the 14th Annual International Cryptology Conference on Advances in Cryptology. 1994: 61-74.

[18] WANG Gui-lin, BAEK J, WONG D S,*et al*. On the generic and efficient constructions of secure designated confirmer signatures[C]// Proc of the 10th International Conference on Practice and Theory in Public-Key Cryptography. Berlin:Springer-Verlag,2007: 43-60.

[19] ZHANG Fang-guo, CHEN Xiao-feng, WEI Bao-dian. Efficient designated confirmer signature from bilinear pairings[C]//Proc of ACM Symposium on Information, Computer and Communications Security. New York:ACM Press, 2008: 363-368.

[20] LIBERT B, QUISQUATER J J. Identity based undeniable signatures [C]//Proc of Topics in Cryptology-CT-RSA. Berlin:Springer,2004: 112-125.

[21] GALBRAITH S D,MAO W. Invisibility and anonymity of undeniable and confrmer signatures[C]//Proc of RSA Conference on the Cryptographers, Track. 2003:80-97.

[22] WANG Gui-lin, XIA Fu-biao, ZHAO Yun-lei. Designated confirmer signatures with unified verification[C]//Proc of the 13th IMA International Conference on Cryptography and Coding. Berlin: Springer-Verlag, 2011: 469-495.