一个可追踪身份的门限属性签名方案*

行韩睿[a]，卢万谊[a]，魏立线[a,b]，韩益亮[a,b]
(武警工程大学 电子技术系 a. 网络与信息安全武警部队重点实验室；b. 网络与信息安全研究所，西安 710086)

摘 要：在基于属性的签名中，签名者的身份是由一系列属性组成的集合来表示且满足匿名性，但同时签名者也可以利用这一特性滥用签名。提出了一个可追踪身份的门限属性签名方案，它利用 PKG 生成的追踪密钥和比特加密的非交互证据不可区分证明，实现了属性签名的可追踪性和不可联系性。方案的安全性基于计算性 Diffie-Hellman 假设，与现有方案相比，公钥长度、私钥长度和签名运算量明显减少，适用于通信网络带宽受限的环境。

关键词：属性签名；可追踪性；不可联系性；计算性 Diffie-Hellman 假设
中图分类号：TP309.1 **文献标志码**：A **文章编号**：1001-3695(2014)01-0206-04
doi:10.3969/j.issn.1001-3695.2014.01.048

Identify traceable threshold attribute-based signature scheme

XING Han-rui[a], LU Wan-yi[a], WEI Li-xian[a,b], HAN Yi-liang[a,b]
(*a. Key Laboratory of Network & Information Security under the Chinese Armed Police Force, b. Institute of Network & Information Security under the Chinese Armed Police Force, Dept. of Electronic Technology, Engineering University of the Chinese Armed Police Force, Xi'an* 710086, *China*)

Abstract: In an attribute-based signature scheme, one's identity is taken the set of attributes and can keep anonymous. But the signer could abuse this signature with the property at the same time. The paper proposed an identity traceable threshold attribute-based signature scheme. By using the traceable key and the non-interactive witness indistinguishable proof of encrypting each bit of identity, the attribute-based signature scheme achieved the traceability and unlingability. The security the scheme was based on the computational Diffie-Hellman assumption. Compared with the existing schemes, the scheme has the shorter public key, private key and the computation of signature, and is fit for the bandwidth-constrained condition.
Key words: attribute-based signature; traceability; unlinkability; computational Diffie-Hellman assumption

0 引言

2005 年，Sahai 等人[1]首次提出基于身份的模糊加密体制，该加密体制将用户的身份由多个描述性的属性来表示。在模糊加密体制中，只有当用户的属性集合和加密属性集的交集满足一个设定的门限值 d 时才能解密。2006 年，Goyal 等人[2]提出了第一个基于属性的加密(attribute-based encryption，ABE)方案，首次将 ABE 分为密钥策略 ABE(key-policy ABE，KP-ABE)和密文策略 ABE(ciphertext-policy ABE，CP-ABE)。2007 年，Bethencourt 等人[3]提出了第一个 CP-ABE 方案。之后，Ostrovsky 等人[4]提出了支持非单调访问结构的 ABE 方案，丰富了访问结构的表达形式。Cheung 等人[5]提出了不使用线性秘密共享的 ABE 方案，但是该方案只支持与运算。

2008 年，Yang 等人[6]提出了基于身份的模糊签名方案，方案借鉴了基于身份的模糊加密思想，是属性签名(attribute based signature，ABS)的雏形。2009 年，Emura 等人[7]提出了基于属性的群签名方案，使用了访问树和哑属性。之后，Li 等人[8]提出的属性签名方案将多个属性分量的签名数据聚合到一起，大大减少了签名数据的长度。基于属性的签名是将签名者的属性作为签名者的身份信息应用于基于身份的签名中，可以隐藏签名者的身份，但同时签名者也可以利用这一特性滥用签名。针对这一问题，Escala 等人[9]提出了可由 PKG 追踪签名者身份的基于属性的签名方案，对于每一个合法的签名，PKG 对应于一个追踪密钥。在需要确定签名者身份的情况下，PKG 可以通过追踪密钥确定签名者的身份，但是对于不知道追踪密钥的其他验证者，则无法确定多个使用相同属性集或访问结构的签名是否由同一签名者签署的。在不需要完全匿名的情况下，可追踪身份的属性签名方案具有广泛应用前景。

门限签名思想是由 Desmedt 等人[10]提出的，它是数字签名体制与门限秘密共享方案相结合的产物。在门限身份签名方案中，签名私钥被分成若干个子密钥，这些子密钥分别被参与签名的成员所拥有，只有参与签名的成员数大于或等于规定的门限值时才能生成签名，验证者可通过公钥来验证签名的有效性。而在门限属性的签名方案中，这些子密钥被参与签名的用户属性所拥有，只有参与的签名属性多于或等于规定的门限值时才能完成签名。门限技术保证了签名密钥的安全，使得签名方案得以更好地发展。

收稿日期：2013-03-19；**修回日期**：2013-04-25 **基金项目**：国家自然科学基金资助项目(61103230，61103231，61272492，61202492)；陕西省自然科学基金资助项目(2011JM8012)

作者简介：行韩睿(1987-)，男，研究生，主要研究方向为信息研究与安全(825742110@qq.com)；卢万谊(1989-)，男，研究生，主要研究方向为应用密码学；魏立线(1966-)，男，教授，主要研究方向为信息安全、密码学；韩益亮(1977-)，男，副教授，主要研究方向为应用密码学.

本文在文献[11]的基础之上,提出了一个可追踪身份的门限属性签名方案。该方案将用户的身份信息嵌入到属性私钥中,通过签名者的属性私钥完成对消息的签名,方案中 PKG 通过生成追踪密钥和利用比特加密的非交互证据不可区分证明(NIWI 证明)实现签名的可追踪性和不可联系性。

1　预备知识

1.1　双线性对

Z_n 表示所有小于 n 的正整数的集合,Z_n^* 表示整数模 n 的乘法群,G 和 G_T 是阶为素数 n 的乘法循环群, g 是 G 的生成元,定义两个群上的双线性映射为 $e:G\times G\rightarrow G_T$ 双线性对满足下面的性质:

a)双线性。$e(g^a,g^b)=e(g,g)^{ab}$,对所有的 $a,b\in Z_n^*$ 均成立。

b)非退化性。g 是 G 的生成元,则 $e(g,g)\neq 1_{G_T}$是 G_T 的生成元。

c)可计算性。存在有效算法来计算 e。

1.2　相关困难假设

1)计算性 Diffie-Hellman 假设给定 q 阶循环群 G,其中 q 为素数,g 是 G 的生成元,$g^a,g^b\in G,a,b\in Z_p$ 是随机选取的,计算 g^{ab}。如果没有能在运算时间 t 内以不可忽略的概率 ε 解决群 G 上的 CDH 问题,则称 CDH 问题在群 G 中是困难的。

2)子群判定假设 设 p、q 为两个大素数,$n=pq$,G 是阶为 n 的乘法循环群。G_p、G_q 分别为 G 的阶为 p、q 的子群。随机选择 $h\in G$ 或 $h\in G_p$,难以判定 $h\in G_p$ 是否成立。

1.3　访问结构(access structure)

设$\{P_1,P_2,\cdots,P_n\}$表示一个主体的集合,称集合 $A\subseteq 2^{\{P_1,P_2,\cdots,P_n\}}$是单调的,如果对于$\forall B,C$,当 $B\in A$ 且 $B\subseteq C$ 时,有 $C\in A$。一个访问结构是$\{P_1,P_2,\cdots,P_n\}$的非空子集 A,即 $A\subseteq 2^{\{P_1,P_2,\cdots,P_n\}}\setminus\{\varphi\}$,$A$ 中的集合称为授权集,不在 A 中的集合称为非授权集。在基于属性的密码方案中,主体就是属性。

1.4　比特加密的非交互证据不可区分证明

2006 年 Groth 等人[12]提出了一个有效的统计零知识证明系统,并证明其是正确的、完备的,且是证据不可区分的。该证明系统如下:

a)公共参数。设 p、q 为两个大素数,$n=pq$,$e:G\times G\rightarrow G_T$ 为双线性对映射,其中 G 和 G_T 是两个阶为 n 的乘法循环群。G_q 为 G 的阶为 q 的子群。随机选取 G 的生成元 g 以及 G_q 的生成元 h。输出公共参数 $\sigma=(n,G,G_T,e,g,h)$。

b)承诺。对于 1 bit 的消息 $m\in\{0,1\}$,随机选取 $r\in Z_n$,输出承诺 $c=g^mh^r$。

c)证据。输入(σ,c,m,r),对承诺 $c=g^mh^r$,输出其证据 $\pi=(g^{2m-1}h^r)^r$。

d)验证。输入(σ,c,π),验证等式 $e(c,\frac{c}{g})=e(h,\pi)$是否成立。如果等式成立,则输出 1;否则输出 $\perp$。

2　形式化定义和安全模型

2.1　形式化定义

可追踪身份的基于属性签名(traceable-ABS)方案由以下五个算法组成:

a)系统建立。输入安全参数,输出公共参数 PK、主密钥 MSK,追踪密钥 MTK。

b)密钥生成。输入用户身份 u、属性集合 Ω、公共参数 PK 和主密钥 MSK,输出私钥 SK。

c)签名。输入签名属性集合 S、用户私钥 SK 和消息 m,输出签名 σ。

d)验证。输入消息 m 和签名 σ,返回是否接收此签名。

e)追踪。输入签名 σ 和追踪密钥 MTK,输出签名者的身份 u。

2.2　不可联系性

不可联系性(unlinkability)是指给出两个使用相同签名属性集或访问结构所签发的合法签名,敌手在不知道追踪密钥的情况下,即使知道签名者私钥也无法区别这两个签名是否是由同一个签名者所签署的。

2.3　不可伪造性

不可伪造性(unforgeability),即如果不知道签名者的私钥,且没有询问过该签名者对消息 m 关于签名属性集 S 所做的签名,则敌手不能伪造该签名者关于签名属性集 S 的消息签名对(m,S,σ)。

一个基于属性的签名方案,在选择属性集和选择消息攻击模式下,如果不存在多项式时间内的敌手能以不可忽略的优势 ε 赢得以下游戏,则称一个基于属性的门限签名方案具有适应性选择消息和选择属性集攻击模型下的不可伪造性。该游戏在敌手 A 和挑战者 C 之间进行,攻击游戏如下:

a)系统初始化。首先敌手 A 声明他要挑战的签名属性集 S 或访问结构。

b)系统参数设置。挑战者 C 运行系统参数生成算法,得到系统公共参数 PK、主密钥 MSK 和追踪密钥 MTK,并将公共参数 PK 发送给敌手。

c)询问。敌手 A 向挑战者 C 自适应作一系列不同的询问,询问可以根据前面已询问的结果进行。询问方式包括密钥询问、签名询问和追踪询问。其中,在对用户 u 和属性集 Ω 进行密钥询问时,要求不存在签名属性集 $S\subseteq\Omega$。

d)伪造。敌手 A 输出消息签名(m^*,u^*,S^*,σ^*),若以下条件成立,则攻击成功:

(a)$\mathrm{Verify}(\mathrm{PK},m^*,u^*,S^*,\sigma^*)=\mathrm{Valid}$;

(b)A 未对用户 u^* 进行密钥询问;

(c)A 未对用户 u^* 进行密钥询问,A 未对用户 u^* 询问过关于消息 m^*、签名属性 S^* 的签名。

3　方案描述

3.1　新的可追踪身份的门限属性签名方案

本文提出的可追踪身份的门限属性签名方案由五个多项式算法构成,具体算法如下:

a)系统建立(setup)。设 p、q 为两个大素数,$n=pq$,$e:G\times G\rightarrow G_T$ 为双线性对映射,其中 G 和 G_T 是两个阶为 n 的乘法循环群。设 $S\in Z_n$,定义拉格朗日系数 $\Delta_{i,S}(x)=\prod_{j\in S,\,j\neq i}\frac{x-j}{i-j}$。系统支持的属性集合为 Z_n^*,定义 $K=\{1,2,\cdots,k,k+1\}$,对 $i\in$

K,随机选择 $t_i \in G$,定义 $T(X) = g_2^{Xk} \prod_{i=1}^{k+1} t_i^{\Delta_{i,k}(X)}$。定义门限为 d,即用户至少有 d 个属性才可以签名。PKG 随机选择 G 的生成元 g,并随机选择 $\alpha \in Z_n^*$,令 $g_1 = g^\alpha$,同时随机选择 G 中的元素 g_2。G_q 是 G 的阶为 q 的子群,PKG 随机选择 G_q 的生成元 h。此外,随机选择 G 的生成元 u' 以及长度为 n_u 的向量 $U = \{u_i\}$,其中,u_i 为 G 的生成元。则公共参数 PK = $(d, g, g_1, g_2, h, t_1, \cdots, t_{k+1}, e, u', U)$,主密钥 MSK = α,追踪密钥 MTK = q。设用户 u 为长度 n_u 的比特串,令 u 中比特值为 1 的集合 U,则 $U \subseteq \{1, 2, \cdots, n_u\}$,定义 $W(u) = \mu' \prod_{i \in U} \mu_i$。

b)密钥生成(keygen)。当签名者 U 提供签名属性集 $S = \{S_1, \ldots, S_l\}$ 时,PKG 选择一个线性秘密共享方案访问结构 (M, ρ),其中 M 是一个 $l \times n$ 的矩阵,单调函数 ρ 将矩阵 M 的行标号和用户属性相关联,即一个属性最多和矩阵的一行相对应。随机选择 $v_2, \cdots, v_n \in Z_n$,取秘密分享向量 $v = (\alpha, v_2, \cdots, v_n)^T$,其中 α 为秘密分享值,通过计算 Mv 获得 l 个秘密分享值,并把 $\lambda_i = (Mv)_i$ 发送给 $\rho(i)$。对每个属性 S_i,PKG 随机选择 $r_i \in Z_n^*$,生成密钥 $SK_i = (d_{i,0}, d_{i,1}) = (g_2^{\lambda_i} T(i)^{r_i}, g^{r_i})$,并发送给签名者 U。

c)签名(sign)。用户 u 对消息 m 签名,签名

属性集 $S = \{S_1, \cdots, S_l\}$,签名私钥 $SK_S = (SK_i)_{i \in S} = (d_{i,0}, d_{i,1})_{i \in S} = (g_2^{\lambda_i} T(i)^{r_i}, g^{r_i})_{i \in S}$,签名算法执行如下:

(a)对 u 的每一个比特值 $u[i]$ $(i = 1, 2, \cdots, n_u)$,随机选取 $\theta_i \in \mathbf{Z}_n$,计算 $c_i = u_i^{u[i]} h^{\theta_i}$,$\pi_i = (u_i^{2u[i]-1} \times h^{\theta_i})^{\theta_i}$。其中,$c_i$ 是 $u[i] \in \{0, 1\}$ 的承诺,π_i 是 c_i 的证据。签名者计算 $\theta = \sum_{i=1}^{n_u} \theta_i$,$c = u' \prod_{i=1}^{n_u} c_i = (u' \prod_{i=1}^{n_u} u_i^{u[i]}) h^\theta = (u' \prod_{i \in U} u_i) h^\theta = W(u) h^\theta$。

(b)随机选择 $r' \in Z_n^*$,计算 $\sigma_1 = g^{r'}$。

(c)计算 $\sigma_{2,i} = d_{i,0} \times g_1^{mcr'} = g_2^{\lambda_i} T(i)^{r_i} g_1^{mcr'}$。

(d)令 $\sigma_{3,i} = d_{i,1} = g^{r_i}$, 最终输出签名

$\sigma = (\sigma_1, \{\sigma_{2,i}, \sigma_{3,i}\}_{i \in S}, c_1, \cdots, c_{n_u}, \pi_1, \cdots, \pi_{n_u})$

d)验证(verify)。当验证者得到签名 $\sigma = (\sigma_1, \{\sigma_{2,i}, \sigma_{3,i}\}_{i \in S}, c_1, \cdots, c_{n_u}, \pi_1, \cdots, \pi_{n_u})$。验证者验证如下:

(a)选取属性集 $\omega \in S \cap R$,且 $|\omega| \geq d$,其中 R 为验证者属性集。如果 $\{\lambda_i\}$ 是由矩阵 M 算出的秘密值 α 的合法分享值,则存在 $\sum_{i \in \omega} \omega_i \lambda_i = \alpha$。

(b)计算 $c = u' \prod_{i=1}^{n_u} c_i$,并且对所有的 $i = 1, 2, \cdots, n_u$,验证 $e(c_i, u_i^{-1} c_i) = e(h, \pi_i)$ 是否成立。若成立,说明对所有的 $u[i] \in \{0, 1\}$,有 $c_i = u_i^{u[i]} h^{\theta_i}$ 成立 ,则验证者计算出的 c 具有正确的格式。

(c)验证等式 $\prod_{i \in \omega} \left(\frac{e(g, \sigma_{2,i})}{e(g_1^{cm}, \sigma_1) e(T(i), \sigma_{3,i})} \right)^{\omega_i} = e(g_2, g_1)$ 是否成立。若成立,则接收签名;否则拒绝签名。

e)追踪(trace)。PKG 首先验证签名是合法的,然后对所有的 $i = 1, 2, \cdots, n_u$,计算 $(c_i)^q$。若 $(c_i)^q = g^0$,则 $u[i] = 0$;若 $(c_i)^q = (u_i)^q$,则 $u[i] = 1$,从而可以恢复签名者的身份 u。由于对身份 u 的每一个比特 $u[i]$,有等式 $e(c_i, u_i^{-1} c_i) = e(h, \pi_i)$ 成立,则此 Trace 算法正确,使 PKG 实现了对用户身份的追踪。

3.2 正确性

$$\prod_{i \in \omega} \left(\frac{e(g, \sigma_{2,i})}{e(g_1^{cm}, \sigma_1) e(T(i), \sigma_{3,i})} \right)^{\omega_i} = \prod_{i \in \omega} \left(\frac{e(g, g_2^{\lambda_i} T(i)^{r_i} g_1^{mcr'})}{e(g_1^{cm}, \sigma_1) e(T(i), \sigma_{3,i})} \right)^{\omega_i} =$$

$$\prod_{i \in \omega} \left(\frac{e(g, g_2^{\lambda_i} T(i)^{r_i} g_1^{mcr'})}{e(g_1^{cm}, g^{r'}) e(T(i), g^{r_i})} \right)^{\omega_i} =$$

$$\prod_{i \in \omega} \left(\frac{e(g, g_2^{\lambda_i}) e(g, T(i)^{r_i}) e(g, g_1^{mcr'})}{e(g_1^{cm}, g^{r'}) e(T(i), g^{r_i})} \right)^{\omega_i} =$$

$$\prod_{i \in \omega} \left(\frac{e(g, g_2^{\lambda_i}) e(g, T(i)^{r_i}) e(g, g_1^{mcr'})}{e(g_1^{cmr'}, g) e(T(i)^{r_i}, g)} \right)^{\omega_i} =$$

$$e(g_1, g_2)$$

4 安全性及性能分析

本章从方案的不可联系性和不可伪造性对方案的安全性进行分析,并与文献[11]在性能上进行分析比较。

4.1 不可联系性

对于乘法循环群 G,如果子群判定假设成立,则本文的方案满足不可联系性。因为用户 u 的签名 $\sigma = (\sigma_1, \{\sigma_{2,i}, \sigma_{3,i}\}_{i \in S}, c_1, \cdots, c_{n_u}, \pi_1, \cdots, \pi_{n_u})$,其中 $\sigma_1 = g^{r'}$ 是随机的。对于 $\{\sigma_{3,i}\}_{i \in S}$ 中每一个 $\sigma_{3,i}$ 都被 r_i 随机化,因此每一个 $\sigma_{3,i}$ 都是随机的。而对于每一个 $\sigma_{2,i}$,由于 r_i 和 r' 都为随机数,因此每一个 $\sigma_{2,i}$ 也是随机的。根据子群判定的假设,对所有的 $i = 1, \cdots, n_u$,c_i 是 u_i 的承诺,π_i 是 c_i 非交互证据不可区分的证据。因此,(c_i, π_i) 是不会泄露 $u_i \in \{0, 1\}$ 的任何信息,所以本文的方案满足不可联系性。

4.2 不可伪造性

方案的安全性归结为 CDH 问题。模拟器设 p、q 为两个大素数,$n = pq$,G 和 G_T 是两个阶为 n 的乘法循环群,挑战者的挑战属性集为 S。令 $l_u = 2(q_k + q_s)$,随机选择整数 k_u $(0 \leqslant k_u \leqslant n_u)$,对于给定的 q_k、q_s、n_u、$l_u(n_u + 1) < p$。随机选择 $x' \in Z_{l_u}$,$y' \in Z_p$,n_u 维向量 $X = (x_i) \in Z_{l_u}^{n_u}$ 和 $Y = (y_i) \in Z_{l_u}^{n_u}$。对 $i = 1, 2, \cdots, k+1$,令 $t_i = g_2^{\varphi(i)} g^{f(i)}$ ($\varphi(i)$ 为一个 k 次多项式),则 $T(i) = g_2^{ik + \varphi(i)} g^{f(i)}$。定义函数 $F(u) = x' + \sum_{i \in U} x_i - l_u k_u, J(u) = y' + \sum_{i \in U} y_i$,模拟器设置如下公共参数并发送给敌手,令 $g_1 = g^a$,$g_2 = g^b$, $u' = g_2^{-l_u k_u + x'} g^{y'}$, $u_i = g_2^{x_i} g^{y_i}$, $1 \leqslant i \leqslant n_u$,则 $W(u) = u' \prod_{i \in U} u_i = g_2^{F(u)} g^{J(u)}$。

在密钥询问阶段,挑战者 B 不知道密钥,B 应答敌手 A 对密钥提取询问 $SK_i = (d_{i,0}, d_{i,1}) = (g_2^{\lambda_i} (g_1^{-f(i)/(ik+\varphi(i))} (g_2^{ik+\varphi(i)} g^{f(i)})^{r'_i})^{\Delta_{0,S(i)}}, g_1^{-1/(ik+\varphi(i))} g^{r'_i})^{\Delta_{0,S(i)}})$。由于

$d_{i,0} = g_2^{\lambda_i} (g^{-f(i)/(ik+\varphi(i))})_1 (g_2^{ik+\varphi(i)} g^{f(i)})^{r'_i})^{\Delta_{0,S(i)}} = g_2^{\lambda_i} T(i)^{r_i}$

$d_{i,1} = g_1^{-1/(ik+\varphi(i))} g^{r_i'})^{\Delta_{0,S(i)}} = g^{r_i}$,故 $SK_i = (d_{i,0}, d_{i,1})$

为一有效的密钥对。

在签名询问阶段,敌手对消息 m 在挑战者的属性集 S 进行一系列签名询问,挑战者执行密钥生成算法生成签名密钥 SK_i,然后对询问的消息 m 运行签名算法,并将生成的有效签名发送给敌手。

当敌手 A 对属性集 S' $(S' \notin S$ 且 $S' \cap S = \varnothing)$ 进行消息签名时,敌手产生一对有效的签名 $\sigma = (\sigma_1, \{\sigma_{2,i}, \sigma_{3,i}\}_{i \in S'}, c_1, \cdots, c_{n_u}, \pi_1, \cdots, \pi_{n_u})$,模拟器输出 $\prod_{i \in \omega} \left(\frac{e(g, \sigma_{2,i})}{e(g_1^{cm}, \sigma_1) e(T(i), \sigma_{3,i})} \right)^{\omega_i} = e(g_2, g_1) = e(g^{ab}, g)$。当敌手以不可忽略的概率赢得签名伪造,则敌手可以解决 CDH 问题,而由于 CDH 是一个困难问题,因此方案存在不可伪造性。

4.3 性能分析

设 p 表示双线性对运算,e 表示指数运算,$|G|$ 和 $|G_q|$ 分别表示相应群中元素的长度,n 表示属性集的最大属性的个数,

n_m 表示明文长度,n_u 表示用户身份长度,本方案与 Zhang 方案[11]具体比较如表 1 所示。

表 1　方案间公、私钥和签名长度的比较

方案	公钥长度	私钥长度	签名长度
文献[11]	$Z_q^* + \|G_q\| + (n_u + k + 5 + n_m)\|G\|$	$(2n+1)\|G\| + \|G_q\|$	$(n+3)\|G\| + 2n_u\|G_q\|$
本方案	$Z_q^* + \|G_q\| + (n_u + k + 5)\|G\|$	$2n\|G\|$	$(2n+1)\|G\| + 2n_u\|G_q\|$

由表 1 可知,本文方案与文献[11]相比,公钥长度和私钥长度明显减少,这在当今网络资源带宽受限的情况下具有明显的优势,非常适合当今社交网络和车载网络等环境下使用。

由表 2 可知,本文方案与文献[11]相比,验证运算量虽然有所增加,但签名运算量降低了,在当今无线网络等小型网络快速发展的情况下,该方案有着明显的优势。

表 2　运算效率的比较

方案	签名运算量	验证运算量
文献[11]	$(5n_u + 2n + 9/2)e$	$(k+3)e + (n+4)p$
本方案	$(5n_u + n + 1)e$	$(k+3+3n)e + (3n+1)p$

5　结束语

本文在文献[11]的基础上,提出了一个新的可追踪身份的门限属性签名方案。方案的安全性基于一般的计算性 Diffie-Hellman 问题,由 PKG 产生的追踪密钥,实现对属性签名中签名者身份的可追踪性和不可联系性。方案的验证运算效率有所降低,但方案的公钥、私钥有明显的减少,签名效率很大提高,在通信带宽受限的情况下,有明显的优势。

参考文献:

[1] SAHAI A, WATERS B. Fuzzy identify-based encryption[C]//Proc of the 24th Annual International Conference on Theory and APPlications of Cryptographic Techniques. 2005: 457-473.

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

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

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

[5] 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.

[6] YANG pi-yi, CAO Zhen-fu, DONG Xiao-lei. Fuzzy identify based signature with applications to biometric authen tication[J]. Computer and Electrical Engineering, 2011, 37(4): 532-540.

[7] EMURA K, MIYAJI A, OMOTE K. A dynamic attribute- based group signature scheme and its application in an anonymous survey for the collection of attribute statistics[C]// Proc of International Conference on Availability, Reliability and Security. 2009: 487-492.

[8] LI J, AU M H, SUSILO W, *et al*. Attribute-based signature and its applications[C]// Proc of the 5th ACM Symposium on Information, Computer and Communications Security. Beijing: ACM Press, 2010: 60-69.

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

[10] DESMEDT Y, FRANKEL Y. Shared gengration of authenticators and signatures[C]//Proc of Advances in Crypto. Berlin: Springer- Verlag, 1992.

[11] 张秋璞,徐震,叶顶锋. 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.

[12] GROTH J, OSTROVSKY R, SAHAAI A. Perfect noninteractive zero knowledge for NP[C]// Proc of Advances in Cryptology Eurocrypt. Berlin: Springer- Verlag, 2006: 339-358.

(上接第 198 页)

[2] AJTAI M. Generating hard instances of lattice problems[C]//Proc of the 28th Annual ACM Symposium on Theory of Computing. New York: ACM Press, 1996: 99-108.

[3] AJTAI M, DWORK C. A public-key cryptosystem with worst-case/ave rage-case equivalence [C]//Proc of the 29th Annual ACM Symposium on Theory of Computing. New York: ACM Press, 1997: 284-293.

[4] AJTAI M, DWORK C. The first and fourth public-key cryptosystems with worst-case/average-case equivalence [C]//Proc of Electronic Colloquium on Computational Complexity. 2007: 97-134.

[5] GOLDREICH O, GOLDWASSER S, HALEVI S. Public-key cryptosystems from lattice reduction problems[C]//Advances in Cryptology. Berlin: Springer, 1997: 112-131.

[6] HOFFSTEIN J, HOWGRAVE-GRAHAM N, PIPHER J, *et al*. NTRUS: digital signatures using the NTRU lattice[C]//Topics in Cryptology. Berlin: Springer, 2003: 122-140.

[7] PEIKERT C. Public-key cryptosystems from the worst-case shortest vector problem[C]//Proc of the 41st Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2009: 333-342.

[8] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[J]. Journal of the ACM, 2009, 56(6): 34.

[9] MICCIANCIO D, REGEV O. Lattice-based cryptography[M]//Post-Quantum Cryptography. Berlin: Springer, 2009: 147-191.

[10] REGEV O. Lattice-based cryptography[C]//Advances in Cryptology. Berlin: Springer, 2006: 131-141.

[11] KAWACHI A, TANAKA K, XAGAWA K. Multi-bit cryptosystems based on lattice problems[C]//Public Key Cryptography. Berlin: Springer, 2007: 315-329.

[12] AGRAWAL S, BONEH D, BOYEN X. Efficient lattice (H) IBE in the standard model[C]//Advances in Cryptology. Berlin: Springer, 2010: 553-572.

[13] ALWEN J, PEIKERT C. Generating shorter bases for hard random lattices[J]. Theory of Computing Systems, 2011, 48(3): 535-553.

[14] CAI Jin-yi, CUSICK T W. A lattice-based public-key cryptosystem [C]//Selected Areas in Cryptography. Berlin: Springer, 1999: 219-233.

[15] PAN Yan-bin, DENG Ying-pu. A ciphertext-only attack against the Cai-Cusick lattice-based public-key cryptosystem[J]. IEEE Trans on Information Theory, 2011, 57(3): 1780-1785.