标准模型下可审计的基于属性的签名方案

任 燕
(运城学院应用数学系 运城 044000)

摘 要 在基于属性签名方案中,需要一个被称为属性中心的可信方来为用户生成和分发私钥,由于属性中心可以为任意用户计算私钥,因此它必须完全可信。而在很多应用场景下,用户不希望系统中存在一个必须无条件信任的可信中心,因为在这样的系统中,一个恶意的属性中心可以伪造系统中任意用户的签名,甚至可以恶意地分发用户的私钥。为了缓解这个密钥托管问题,可以将可审计的思想引入到基于属性的签名方案中,并在标准模型下构造一个可审计的基于属性的签名方案。最后证明了该方案的安全性。

关键词 基于属性签名,可审计,标准模型

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.2.031

Attribute-based Signatures with Auditabiling in Standard Model

REN Yan
(Department of Applied Mathematics, Yuncheng University, Yuncheng 044000, China)

Abstract In an ABS scheme, the attribute authority (A-authority) generates the private key for any users, hence it has to be completely trusted. The A-authority is free to engage in malicious activities without any risk of being confronted in a court of law. Motivated by this, we firstly proposed a notion of audit attribute-based signature scheme. It is not only a variant of ABS, but also a new approach to mitigate the key escrow problem. Then we constructed a audit attribute-based signature scheme in the standard model. Finally, we proved its security under the standard model.

Keywords Attribute-based signature, Audit, Standard model

1 引言

Sahai 和 Waters[1]在 2005 年第一次提出属性的概念,之后基于属性的数字签名体制的思想由基于模糊身份签名[2]的概念发展而来,从此,基于属性的签名方案成为研究热点[3-10]。在基于属性签名的方案中,由于用户自己不能为自己的属性集合生成私钥,因此需要一个被称为属性中心的可信方来为用户生成和分发私钥。由于属性中心可以为任意用户计算私钥,因此它必须完全可信。而在很多应用场景下,用户不希望系统中存在一个必须无条件信任的可信中心,因为在这样的系统中,一个恶意的属性中心可以伪造系统中任意用户的签名,甚至可以恶意地分发用户的私钥。因此,研究无密钥托管的基于属性签名体质或减轻基于属性签名体制的密钥托管问题的机制都将是很有意义的工作。

目前,为了解决秘钥托管问题,在基于属性签名的方案中,可以采取多个属性中心来为用户生成秘钥[11-14]。在多属性中心的方案中,存在多个属性,每个属性中心负责为属性集合的一个子集生成私钥,即一个用户得到几个私钥,而其中的每一个都来自一个不同的属性中心。而对于多属性中心的基于属性的签名,一个重要的问题是它不能抵抗合谋攻击。同时,还有一个问题是:在现有的多属性中心的属性签名方案中,都需要在多个属性中心中增加一个关于属性集合的特殊的中枢中心。如果这个中枢中心是恶意的,则系统的安全性全部被攻破。T. Okamoto 等[14]证明了如果中枢中心被收买,在文献[12]中的多属性中心的方案都是不安全的。而现在,无中枢中心的多属性中心的属性签名还未被提出。

本文通过扩展 Goyal 在文献[15]中关于基于身份的加密(Identity-based encryption, IBE)所提出的可审计的思想,利用他们提出的追踪算法,在标准模型下提出了可审计的基于属性的签名方案。

可审计中心的基于属性的签名的形式是:

1. 在一个可审计中心的基于属性签名方案中,对于每个用户有指数数量的可能的私钥。

2. 通过运行一个交互的秘钥生成协议,一个用户可以从属性中心获得对应于他的属性的私钥。这个协议还允许用户获得一个单一的属性中心不知道的秘钥族。然后,用户可以为他的属性计算一个属于秘钥族的私钥。

3. 用户不能发现和计算不属于同一秘钥族的其他的私钥。

4. 如果属性中心恶意地为属性生成一个秘钥族和一个私钥,它们与用户得到的秘钥族和私钥是不同的。

在这种情形下,属于不同秘钥族的两个不同的私钥是属性中心恶意行为的一个证明。属性中心只能被动地伪造用户的签名。用户可以通过将秘钥族提供给法院作为控告属性中

到稿日期:2014-03-26 返修日期:2014-05-19 本文受国家自然科学基金(11241005),生物数学重点实验室开放课题(SWSX201306)资助。
任 燕(1982—),女,博士生,主要研究方向为密码学、信息安全。

心的证据。这意味着如果属性中心恶意地伪造用户的签名将有非常巨大的风险。本方案中，在需要的时候可以追踪到到底是用户还是属性中心完成的签名。

2 预备知识

2.1 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 $e:G_1\times G_1\rightarrow G_2$ 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 $P,Q\in G_1$ 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 $e(P,Q)$。

2.2 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$(x_i,f(x_i))$，则通过式(1)能唯一确定任意一个 x 所对应的多项式 $f(x)$值：

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

对于式(1)，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：

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

2.3 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)计算 Diffie-Hellman 问题假设 (CDH)。

设 G 是一个阶为素数 p 的循环群，对于 $g,g^a,g^b\in G$，不存在多项式时间的算法可以以不可忽略的优势计算出 $g^{ab}\in G$，这里 $a,b\in Z_p$。

3) 修改的计算 Diffie-Hellman 问题假设 (MCDH)。

给定 $g,g^a,g_1\in G$，不存在多项式时间的算法可以以不可忽略的优势计算出 $g_1^{\frac{1}{a}}\in G$，这里 $a\in Z_p$。

3 方案的定义和安全模型

3.1 定义

定义 1 一个可审计中心的基于属性的签名方案由初始化算法 Setup、秘钥生成算法 Keygen、签名算法 Sign、验证算法 Verify 和追踪算法 Trace 组成。

令 w 是可能的属性集合，w 上的一个断言实际上是一个输入为关于属性 w 的布尔函数。当 $\gamma(w)=1$ 时，我们称属性集合 $w'\subseteq w$ 满足一个断言 γ。各个算法的描述如下：

1)Setup：该算法的输入为安全参数 k，输出为系统的主公钥 pk 和主私钥 mk。

2)Keygen：属性中心与用户 U 合作执行一个交互协议。属性中心和 U 的公共输入为主公钥 pk 和 U 的属性集合 w。中心的私有输入为主私钥 mk。此外，还可能包括用于属性中心和 U 的私有输入的随机值。在协议的最后，用户 U 可以获得一个私钥 d_w 作为他的私有输出。任何时间任意一方可以终止该协议。

3)Sign：输入为系统参数、断言 γ、满足的属性集合 $\gamma(w)=1$，$w'\subseteq w$，属性秘钥 d_w 和消息 m，输出为签名者对消息 m 的签名 σ。

4)Verify：输入为系统参数、消息 m、对消息的签名 σ 和满足断言 γ 的属性 w，在 σ 是消息 m 和满足 $\gamma(w)=1$ 的有效签名时，该算法的输出为 true。

5)Trace：输入秘钥族和签名 σ，输出为 0 或者 1，输出为 0 表示消息 m 的签名是由属性中心完成的。而输出是 1 则表示消息 m 的签名是由用户完成的。

3.2 安全模型

我们修改 Goyal 在文献[15]中提出的关于 IBE 的安全模型。类似地，我们给出下面 3 个游戏。

3.2.1 伪造游戏

不可伪造性的定义依赖于下面的游戏。这个游戏包括一个挑战者 C 和一个敌手 A。该游戏描述如下：

1. Setup：挑战者 C 选择一个安全参数，运行可审计中心的基于属性的签名方案的 Setup 算法。然后，挑战者 C 获得主密钥 sk 和公共参数 pk，挑战者保存密钥，将公共参数发给敌手 A。

2. Keygen：敌手 A 与挑战者 C 运行关于属性集合 w 密钥生成协议，挑战者 C 用密钥 sk 应答。

3. Query：敌手 A 可以对签名预言进行多项式次数的查询，挑战者 C 用密钥 sk 应答。

4. Forgery：最后，敌手 A 输出签名关于消息 m^* 的签名 σ^*。

若敌手输出的签名 σ^* 是消息 m^* 关于断言 γ 的有效签名，这里 m^*，σ^* 在签名预言阶段未被查询且没有属性 w^* 使得 $w\subseteq w^*$ 和 $\gamma(w)=1$ 同时满足，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，则一个可审计的基于属性的签名方案是不可伪造的。

3.2.2 寻找密钥游戏

这个游戏包括一个挑战者 C 和一个敌手 A。挑战者 C 和敌手 A 都以安全参数作为输入。该游戏描述如下：

1. Setup：敌手 A(可以是一个恶意的属性中心)生成和分发公共参数 pk 给挑战者 C。

2. Keygen：敌手 A 与挑战者 C 运行关于属性集合 w 的密钥生成协议，如果没有一方终止协议，则挑战者 C 得到秘钥 d_w 作为输出并对它进行一次健全性验证以确保它是良好生成的。如果验证失败则终止。

3. Find Key：敌手 A 输出密钥 d_w'，挑战者 C 对它进行一次健全性验证，如果验证失败则终止。如果 d_w'和 d_w 是属于同一秘钥族的不同的私钥，且 $trace(d_w')=trace(d_w)$，则敌手赢得游戏。

3.2.3 计算新密钥游戏

计算新密钥游戏描述如下：

1. Setup：挑战者 C 运行可审计中心的基于属性的签名方案的 Setup 算法。然后，挑战者 C 将公共参数发给敌手 A。

2. Keygen：敌手 A 与挑战者 C 运行关于自适应选择的属性集合 $w_1,w_2,\cdots,w_q$ 密钥生成协议，然后得到私钥 d_{w_1}，$d_{w_2},\cdots,d_{w_q}$。

3. New Key Computation：敌手 A 为一个属性集合 w 输出两个密钥 d_{w_1} 和 d_{w_2}。挑战者 C 对两个秘钥进行一次健全性验证，如果验证失败则终止。

如果 d_{w_1} 和 d_{w_2} 是属于不同秘钥族的不同的私钥，且 $trace(d_{w_1})=trace(d_{w_2})$，则敌手赢得游戏。

定义 3 如果对任意多项式时间的敌手 A 至多只能以可忽略的优势赢得上述的伪造游戏、寻找密钥游戏和计算新密钥游戏，则称可审计的基于属性的签名方案是安全的。

4 方案的构造

本文的标准模型下可审计的基于属性的签名方案支持所有包含门限门的断言 γ。特别地，对所有的具有门限值 d 的 w^* 有

$$\gamma_{d,w^*}(w')=\begin{cases}1, & |w'\cap w^*|>d\\ 0, & \text{其他}\end{cases}$$

1)初始化(SetUp)

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。初始化阶段由以下几步完成：

首先定义属性集合 U，为简单起见，我们可以取 Z_p 的前 l 个元素来做为这个集合，即：$1,\cdots,l(\mathrm{mod}p)$；

然后随机选取 $x,y\in Z_p$，计算 $X=g^x,Y=g^y$。并随机选 $g_1,g_2\in G_1$。从群 G_1 均匀随机选择 $t_1,\cdots,t_{n+1}$。令 $N=\{1,\cdots,n+1\}$，我们定义一个函数 T，如下所示：

$$T(x)=g_2^{x^n}\prod_{j=1}^{n+1}t_j^{\Delta_{j,N}(x)}$$

最后，从 Z_p 中随机选择一个 u'，从 Z_p^k 中选择一个随机向量 $u=(u_1,\cdots,u_k)$。

则公共参数为：$G_1,e,g,g_1,g_2,g_3,X,Y,u,t_1,\cdots,t_{n+1}$。

主密钥为：x,y。

2)密钥生成协议(Key Generation Protocol)

属性中心和拥有属性 w 的用户 U 之间的密钥生成协议按如下进行。

U 随机选取 $s_0\in Z_p$，并将 $R=g_1^{s_0}$ 发送给属性中心。同时，U 给出离散对数 $\log_R g_1$ 的零知识证明。

属性中心随机选择 $s_1,r',r_i\in Z_p$ 和一个 $d-1$ 阶的多项式 $q(\cdot)$ 满足 $q(0)=x$。然后，计算如下值：

$$d_u'=(d_1',d_2',d_3',d_4')$$

$$=((YRg_1^{s_1})^{\frac{1}{x}}g_2^{r'},s_1,\{D_i=g_2^{q(i)}XT(i)^{r_i}\},\{F_i=g^{r_i}\})$$

将它们发送给用户 U 并公开 $X^{r'}$。

U 随机选取 $r''\in Z_p$ 并计算：

$$d_w=(d_1,d_2,d_3,d_4)$$

$$=(d_1'g_2^{r''},d_2'+s_0,d_3',d_4')$$

$$=((YRg_1^{s_1})^{\frac{1}{x}}g_2^{r},s,\{D_i=g_2^{q(i)}XT(i)^{r_i}\},\{F_i=g^{r_i}\})$$

这里 $s=s_0+s_1,r=r'+r''$。然后公开 X^r。

U 按照如下方式对秘钥 d_w 进行一个健全性检验：

它选择一个含 d 个元素的子集 $S\subseteq w$ 并计算：$R_i=\frac{e(D_i,g)}{e(F_i,XT(i))}$，$R_0=\prod_{i\in S}R_i^{\Delta_{i,S^{(0)}}}$。

然后它选择一个子集 $T\subseteq S$，且 $|T|=d-1$，令 $S'=T\cup\{0\}$ 并对 $j\in w-S'$ 检验：

$$\prod_{i\in S}R_i^{\Delta_{i,S'(j)}}=\frac{e(D_j,g)}{e(F_j,XT(i))},j\in w-S'$$

最后检验

$$\frac{e(d_1,X)}{e(g,g_1)e(g_2,X^rX^{r'})}=e(g,Y),R_0e(g,Y)=e(g_1,X)$$

如果上述的检验都通过，则说明 U 对它的属性 w 具有一个良好形式的密钥 d_w。

U 设置秘钥族 $n_F=d_2=s$。

3)签名生成(Sign)

假设一个用户对属性 w 有密钥，对消息 $m=(\mu_1,\mu_2,\cdots,\mu_n)\in\{0,1\}^n$ 在断言 $\gamma_{d,w^*}(\cdot)$ 下进行签名(即证明至少拥有 n 元属性集合中的 d 个属性)的过程如下：

选择一个 d 元子集 $w'\subseteq w\cap w^*$。对 $i\in S$ 选择 d 个随机值 $r_i'\in Z_p$，然后计算：

$$\sigma_0=g^s,\sigma_1=g_1^s,\sigma_2=g_2^s,$$

$$\sigma_3=((Y_1g_1^s)^{\frac{1}{x}}g_2^r)^s,$$

$$\sigma_4=\prod_{i\in S}((g_1)^{q(i)}(XT(i))^{r_i})^{\Delta_{i,s^{(0)}}}\prod_{i\in S}(XT(i))^{r_i'}\times(u'\prod u_j^{\mu_j})^s,$$

$$\sigma_i'=(g^{r_i})^{\Delta_{i,S^{(0)}}}g^{r'_i},i\in S$$

输出签名：

$$\sigma=\{\sigma_0,\sigma_1,\sigma_2,\sigma_3,\sigma_4,\{\sigma_i'\}\}$$

4)签名验证(Verify)

可以通过检验如下式子验证签名 $\sigma=\{\sigma_0,\sigma_1,\sigma_2,\sigma_3,\sigma_4,\{\sigma_i'\}\}$ 的有效性是否成立：

$$\frac{e(\sigma_3,X)}{e(\sigma_2,X^rX^{r'})}=$$

$$e(Y\sigma_1,\sigma_0)\frac{e(\sigma_4,g)}{\prod e(XT(i),\sigma_i')e(u'\prod(u_j)^{\mu_j},\sigma_0)}$$

$$=e(g_1,X)$$

5)追踪(Trace)

这个算法以秘钥族 s 和签名 σ 作为输入。然后计算：$\sigma_0=g^s$。若式子成立则输出 1；否则输出 0。

5 方案的正确性和安全性分析

5.1 方案的正确性分析

定理 1 签名的验证过程是正确的。

证明：

$$(1)\frac{e(\sigma_3,X)}{e(\sigma_2,X^rX^{r'})}=\frac{e(((Y_1g_1^s)^{\frac{1}{x}}g_2^r)^s,X)}{e(g_2^s,X^r)}$$

$$=\frac{e(Y^{\frac{s}{x}},X)e(g_1^{\frac{s^2}{x}},X)e(g_2^{rs},X)}{e(g_2^s,X^r)}$$

$$=e(Y^s,g)e(g_1^s,g^s)=e(Y\sigma_1,\sigma_0)$$

$$(2)\frac{e(\sigma_4,g)}{\prod e(XT(i),\sigma_i')e(u'\prod(u_j)^{\mu_j},\sigma_0)}$$

$$=\frac{e(\prod_{i\in S}((g_1)^{q(i)}(XT(i))^{r_i})^{\Delta_{i,s^{(0)}}},g)e(\prod_{i\in S}(XT(i))^{r_i'},g)}{e(\prod(XT(i),g^{r_i\Delta_{i,S^{(0)}}})e(\prod XT(i),g^{r_i'})}$$

$$\frac{e((u'\prod u_j^{\mu_j})^s,g)}{e(u'\prod(u_j)^{\mu_j},g^s)}$$

$$=e((\prod_{i\in S}g_1^{q(i)})^{\Delta_{i,S^{(0)}}},g)$$

$$=e(g_1^s,g)=e(g_1X)$$

5.2 方案的安全性分析

定理 2 我们的方案在 CDH 假设下是不可伪造的。

证明：假设一个敌手可以以 ε 的优势攻破我们的方案，则可以构建一个算法 F 来解决 CDH 问题。

算法 F 在给定 $(g,X=g^x,Y=g^y)$ 时，可计算出 g^{xy}。具

体过程如下：

Setup：

A 输出挑战断言，即至少拥有 n 元属性集合 w^* 中 d 个元素。然后，F 令 $g_1=X$ 和 $g_2=Y$，随机选取 d 个元素，n 个元素 $u_i\in G_1$。

若 $i\in w^*$，则从群 G_1 均匀随机选择 $t_1',\cdots,t'_{n+1}$。令 $N=\{1,\cdots,n+1\}$，$U_i=(u_i)$。

$T(i)=g^{i^n}\prod_{j=1}^{n+1}t_j^{\Delta_{j,N}(i)}$，若 $i\notin w^*$，则令 $U_i=(u_i)=(g^{a_i})$，$T(i)=g^{\beta_i}$，这里的 α_i,β_i 从 Z_p 中随机选取。

KeyGen

A 可以对私钥进行查询。当 F 收到 $R=g_1^{s_0}$ 及关于离散对数 $\log_{g_1}R$ 的零知识证明时，F 按照如下方式模拟生成属性 w 的私钥：

随机选择 $s_1\in Z_p$，令 $s=-\frac{\gamma}{\alpha_i}+s_1$，$W=Y(g_1)^{\frac{-w'}{\alpha_i}}g_1^{s_1}$。

计算 $d_1=g_2^{r'}(X^{-w})=g_2^{r'}W^{-x}$，$\omega=\log_g W$，$d_2=s$。这里 r' 是从 Z_p 中随机选取的。

定义 3 个集合：$\Gamma=w^*\cap w$，Γ' 满足 $\Gamma\subseteq\Gamma'\subseteq w$ 和 $|T'|=d-1$，$S=\Gamma'\cup\{0\}$。F 模拟生成私钥中的 D_i,F_i：

若 $i\in T'$，则 $D_i=g_2^{\tau_i}XT(i)^{r_i}$，$F_i=g^{r_i}$，这里的 τ_i 和 r_i 是从 Z_p 中随机选取的。

若 $i\notin\Gamma'$，则 $D_i=g_2^{\frac{\Delta_{0,S}(i)\gamma_i}{\beta_i}+\sum_{i\in T'}\Delta_{j,S}(i)q(j)}(g_1^{-\beta}g^{\gamma_i})^{r_i'}$，

$F_i=g_2^{\frac{\Delta_{0,S(i)}}{\beta_i}}g^{r_i'}$。

由 $q(i)=\sum_{j\in T'}\Delta_{j,S}(i)q(j)+\Delta_{0,S}(i)q(0)$ 可知，F 正确模拟了私钥。

若令 $r_i=\frac{\Delta_{0,S}(i)}{\beta_i}y+r'_i$，我们有：

$$g_1^{q(i)}(XT(i))^{r_i}=g_2^{\frac{\Delta_{0,S}(i)\gamma_i}{\beta_i}+\sum_{i\in T'}\Delta_{j,S}(i)q(j)}(XT(i))^{r_i'},$$

$$g^{r_i}=g_2^{\frac{\Delta_{0,S}(i)}{\beta_i}}g^{r_i'}$$

Sign Query

A 也可以要求一个属性集合 w 对消息 $m^*=(\mu_1^*,\cdots,\mu_k^*)$ 的签名进行查询。

若 $w\cap w^*\geqslant d$，则 F 可以对 w 通过私钥模拟生成一个模拟的私钥，并正常地得到属性集合 w 对消息 m 的签名。

若 $d\geqslant|w\cap w^*|\geqslant k$，则 F 可以按如下模拟签名：

首先选择一个 $r_i,u'\in Z_p$，$\omega'=\log_g g_2$，$u'\prod u_j^{\mu_j^*}=g_2^{\beta_i'}$，计算：

$$g^s=g_2^{\frac{-1}{\alpha_i}}g^{s_1},g_1^s=g_1^{\frac{-w}{\alpha_i}}g_1^{s_1},$$

$$g_2^s=g_1^{\frac{-w}{\alpha_i}}g_2^{s_1},$$

$$(g_2^{r'}W^{-x})^s=(g_2^{r'}g_1^{-w})^{\frac{-w'}{\alpha_i}}(g_2^{r'}g_1^{-w})^{s_1},$$

$$g_2^r\prod_{i\in S}T(i)^{r_i}(u'\prod u_j^{\mu_j})^s=(g_1^{a_1}g^{\beta_i})^{s_1}\prod_{i\in S}T(i)^{r_i}g_2^{\frac{-\beta_i}{\alpha_i}}$$

最后，敌手输出一个属性集合 w^* 对消息 m^* 的伪造签名：

$$\sigma^*=(\sigma_0^*,\sigma_1^*,\sigma_2^*,\sigma_3^*,\sigma_4^*,\{\sigma_i'^*\})$$

$$=(g^s,g_1^s,(g_2^{r'}W^{-x})^s,g_2^r\prod_{i\in S}T(i)^{r_i}\times(u'\prod u_j^{\mu_j})^s,\{g^{r_i}\})$$

则 F 可计算：$g^{xy}=\frac{\sigma_4^*}{\prod(\sigma_i'^*)^{\beta_i}(\sigma_0^*)^{\beta_i'}}$

下面分析 F 成功的概率：

我们要求伪造的签名满足 $w\cap w^*\geqslant d$，而从 $n-k$ 个元素的集合中正确猜出 $d-k$ 个元素的子集的概率是 $1/C_{n-k}^{d-k}$，所以，F 可以以 $\varepsilon'=\varepsilon/C_{n-k}^{d-k}$ 的优势解决 CDH 问题。

定理 3 在信息论意义下，对本方案来说，一个敌手赢得寻找秘钥游戏的优势是可忽略的。

证明：这个证明可以直接由用户承诺的计算隐藏性质和提供离散对数知识证明协议的证据的计算不可分辨性得到。因为承诺 $R=g^{s_0}$ 和 s_0 的知识证明可以保证对属性中心计算隐藏了 s_0。Z_p 中的所有元素均可以等可能地成为值 $d_2=s_0+s_1$，并将其作为用户最后私钥的最后部分。

定理 4 在 MCDH 假设下，对我们的方案来说，一个敌手赢得计算新秘钥游戏的优势是可忽略的。

证明：假设一个敌手可以攻破我们的方案，则可以构建一个算法 F 来解决 MCDH 问题。算法 F 在给定 $g,X=g^x,g_1$ 时，可计算出 $g_1^{\frac{1}{x}}$。具体过程如下：

Init：敌手宣布攻破目标属性 w^*。

Setup：

F 首先像上述情形设置 X,g_1。然后，F 随机选择 $\alpha,\beta,\rho,s'\in Z_p$，并令：$Y=X^{\rho}(g_1)^{-s'}$，$g_2=X^{\beta}$。最后，输出公共参数。

KeyGen

A 可以对属性 w 的私钥进行请求。

F 将收到 $R=g_1^{s_0}$ 及关于离散对数 $\log_{g_1}R$ 的零知识证明。如果对零知识证明的验证失败，则 F 终止；若验证通过，则 F 按照如下方式模拟生成属性 w 的私钥：

若 $w\neq w^*$，F 按照如下方式完成：

F 随机选择 s_1,r'，设置 $W=YRg_1^{s_1}$。然后计算 $\omega=\log_g W,d_3,d_4$ 如定理 2。

若 $w=w^*$，使用知识提取器，F 可以获得 s_0。然后 F 令 $s_1=s_1'-s_0$ 并以如下方式响应：$(d_1,d_2)=(g^{\rho},s_1),d_3,d_4$ 如定理 2。

NewKeyComputation

这一步通过以下步骤完成：

A 输出两个私钥 $d_w=(d_1,d_2,d_3,d_4),k_w=(k_1,k_2,k_3,k_4)$ 这里 $s=d_2\neq k_2=s'$。

然后我们有：$d_1=(Yg_1^s)^{\frac{1}{x}}X^{\beta r_1}X^{r_1}$，$k_1=(Yg_1^s)^{\frac{1}{x}}X^{\beta r_2}X^{r_2}$，这里的 r_1,r_2 是在 Z_p 中选取的且对 F 是保密的。

最后，F 可以计算：$g_1^{\frac{1}{x}}=(\frac{d_1/X^{r_1\beta}}{k_1/X^{r_2\beta}})^{\frac{1}{s-s'}}$。

下面分析 F 成功的概率：

由于计算新密钥成功要求 $d_1\neq k_1$，而

$$d_1=(Yg_1^s)^{\frac{1}{x}}X^{\beta r_1}X^{r_1}$$

$$k_1=(Yg_1^s)^{\frac{1}{x}}X^{\beta r_2}X^{r_2}$$

所以要求 $r_1\neq r_2$，由于 $r_1=r_2$ 的概率是 $\frac{1}{p-1}$，则 F 可以以 $\varepsilon=1-\frac{1}{p-1}$ 的优势解决 MCDH 问题。

由定理 2－定理 4 我们可以得到如下的定理：

定理 5 我们的可审计中心的基于属性的签名方案在 CDH 和 MCDH 假设下是安全的。

结束语 为了缓解基于属性签名中的密钥托管问题，我们将可审计的思想引入到基于属性的签名方案中，在标准模型下构造了可审计的基于属性的签名方案，并在 CDH 和

MCDH 假设下证明了方案的安全性。

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] Yang P, Cao Z, Dong X. Fuzzy Identity Based Signature with applications to biometric authentication [J]. Computer Electrical Engineering, 2011, 37(4): 532-540

[3] Shaniqng G, Yingpei Z. Attribute-based signature scheme[C]// International Conference on Information Security and Assurance, 2008(ISA 2008). IEEE, 2008: 509-511

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

[5] Li J, Au M H, Susilo W, et al. Attribute-based signature and its applications[C]// Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. ACM, 2010: 60-69

[6] Escala A, Herranz J, Morillo P. Revocable attribute-based signatures with adaptive security in the standard model [M]// Progress in Cryptology-AFRICACRYPT 2011. Springer Berlin Heidelberg, 2011: 224-241

[7] Maji H K, Prabhakaran M, Rosulek M. Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance [OL]. http://eprint.iacr.org/2008/328.pdf

[8] Khader D. Attribute Based Group Signatures [OL]. http://eprint.iacr.org/2007/159.pdf

[9] Khader D. Attribute Based Group Signature with Revocation [OL]. http://eprint.iacr.org/2007/241.pdf

[10] Li J, Kim K. Attribute-Based Ring Signatures [OL]. http://epring.iacr.org/2008/394.pdf

[11] Li J, Huang Q, Chen X, et al. Multi-authority ciphertext-policy attribute-based encryption with accountability[C]// Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security. ACM, 2011: 386-390

[12] Shahandashti S F, Safavi-Naini R. Threshold attribute-based signatures and their application to anonymous credential systems [M]// Progress in Cryptology-AFRICACRYPT 2009. Springer Berlin Heidelberg, 2009: 198-216

[13] Maji H K, Prabhakaran M, Rosulek M. Attribute-based signatures[M]// Topics in Cryptology-CT-RSA 2011. Springer Berlin Heidelberg, 2011: 376-392

[14] Okamoto T, Takashima K. Efficient attribute-based signatures for non-monotone predicates in the standard model[M]// Public Key Cryptography-PKC 2011. Springer Berlin Heidelberg, 2011: 35-52

[15] Goyal V. Reducing trust in the PKG in identity based cryptosystems[M]// Advances in Cryptology-CRYPTO 2007. Springer Berlin Heidelberg, 2007: 430-447

(上接第 136 页)

一个好的入侵检测方案，不仅要尽量提高系统的检测率，而且要尽可能地降低系统的误报率，以提高系统报警的可信度。算法分类准确率比较如表 5 所列，相比于 SK-Means (semi-supervised K-Means)算法[14]和 SFCA(semi-supervised fuzzy clustering algorithm)算法[14]，ML-KNN 算法在标记数据的训练下建立了一个较好的模型。观察图 2 和图 3 可知，随着标记数据比例增加，算法的检测率逐渐提高，误报率明显降低；同时，ML_KNN 在检测率和误报率上明显优于算法 SK-Means 和 SFCA。因此将多标记和半监督学习应用于入侵检测，能够有效改善入侵系统的性能。

结束语 本文提出的方案具有更高的检测率和更低的误报率，实验证明，将多标记学习应用于入侵检测系统，能够很好地改善系统性能，优于传统的入侵检测算法。但本文算法是基于多标记学习 K-NN 算法，因此如何改进使其更适应入侵检测系统是目前有待解决的问题。同时本文对异常记录给予标记偏多，现实网络环境正常记录远远多于异常记录，如何模拟现实网络环境进行基于多标记学习的入侵检测实验也是今后值得考虑的研究方向。

参 考 文 献

[1] Wu Qing-tao, Shao Zhi-qing. Survey on intrusion detection techniques[J]. Application Research of Computers, 2005, 22(12): 11-44

[2] Schapire R E, Singer Y. Boostexter: A boosting-based system foe text categorization [J]. Machine Learning, 2000, 39(2/3): 135-168

[3] 宋相法，焦李成. 基于稀疏编码和集成学习的多示例多标记图像分类方法[J]. 电子与信息学报，2013，35(3)：622-626

[4] 陈晓峰，王士同，曹苏群. 半监督多标记学习的基因功能分析[J]. 智能系统报，2008，3(1)：83-90

[5] 周志华，张敏灵. MIML：多示例多标记学习[J]. 机器学习及其应用，2009：218-234

[6] Zhang Min-ling, Zhou Zhi-hua. A Lazy Learning Approach to Multi-Label Learning [J]. Pattern Recognition, 2007, 40(7): 2038-2048

[7] 周志华，杨强. 机器学习及其应用[M]. 北京：清华大学出版社，2011：179-199

[8] University of California, Irvine. KDD cup 1999 data[EB/OL]. 1999-10-28 [2012-03-20]. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[9] Elisseeff A, Weston J. A kernel method for multi-labelled classification[C]// Dietterich T G, Becker S, Ghahramani Z., eds. Advances in Neural Information Processing Systems 14 (NIPS' 01). Cambridge, MA: MIT Press, 2002: 681-687

[10] 袁利永，王基一. 一种改进的半监督 K-Means 聚类算法[J]. 计算机工程与科学，2011，33(6)：138-143

[11] 夏战国，万玲，蔡世玉，等. 一种面向入侵检测的半监督聚类算法[J]. 山东大学学报：工学版，2012，42(6)：1-7

[12] 郭跃健，李宏. 多值属性和多标记数据分类[D]. 长沙：中南大学，2010

[13] 谢中华. Matlab 统计分析与应用：40 个案例分析[M]. 北京：北京航空航天大学出版社，2010

[14] 王汝山，李永忠. 基于半监督聚类的入侵检测技术研究[D]. 镇江：江苏科技大学，2010