文章编号:2095-6134(2015)05-0708-06

常数签名长度的高效基于属性签名协议设计*

张 严[1†], 张立武[1], 张茉莉[2]

(1 中国科学院软件研究所 可信计算与信息保障实验室, 北京 100190; 2 中国联合网络通信集团有限公司, 北京 100033)

(2014 年 8 月 27 日收稿; 2015 年 5 月 6 日收修改稿)

Zhang Y, Zhang L W, Zhang M L. Efficient attribute – based signature with constant signature size[J]. Journal of University of Chinese Academy of Sciences, 2015,32(5):708-713.

摘 要 作为一种新的密码学工具,基于属性的签名方案使得用户可以使用其属性信息作为公钥进行签名而无需证书绑定.该签名随后可被验证满足特定的访问控制结构,同时不会暴露用户的具体身份和属性信息.上述性质使得基于属性的签名在有效保护用户隐私的同时,实现了基于属性的访问控制,因此得到了许多关注.在本文中,我们对当前基于属性签名方案的效率进行了改进,提出了一个可以实现常数签名长度的门限式基于属性签名方案,并在随机预言机模型下对方案的安全性进行了证明.与现有方案相比,本方案在保持其它参数长度可实用的情况下,缩短了签名长度,提高了通信效率.

关键词 基于属性; 签名方案; 效率

中图分类号:TP391 **文献标志码**:A **doi**:10.7523/j.issn.2095-6134.2015.05.019

Efficient attribute-based signature with constant signature size

ZHANG Yan[1], ZHANG Liwu[1], ZHANG Moli[2]

(1 *Trusted Computing and Information Assurance Laboratory, Insitute of Software, Chinese Academy of Sciences, Beijing* 100190, *China*; 2 *China United Network Communications Corporation Limited, Beijing* 100033, *China*)

Abstract As a new cryptographic tool, attribute-based signature (ABS) allows user to sign messages using his attributes. The signature could be verified to satisfy some predicate without exposing any particular attributes or identity information of the signer. These properties effectively protect user's privacy while achieving attribute-based access control. In this paper, we propose an efficient threshold attribute-based signature scheme with constant signature size and constant pairing computation during verification. The scheme has been proved to be unforgeable and unconditionally anonymous. Compared with other existing constant-size ABS schemes, our scheme is short in signature size while keeps the secret key size acceptable.

Key words attribute-based; digital signature; efficiency

基于属性的密码学概念最初由 Sahai 和 Water[1]提出,是对基于身份密码学的扩展.在文

* 国家自然科学基金(61303247)和国家 863 计划项目(2012AA01A403)资助

† 通信作者,E-mail:zhangyan@tca.iscas.ac.cn

献[1]中,Sahai 和 Water 提出第 1 个基于属性的加密方案,通过将用户身份扩展为描述用户的属性集合,可以实现更为灵活的策略设置. 与基于属性的加密方案相对应,基于身份签名(Identity-based Signature, IBS)文献[2]的类似扩展被称为基于属性的签名(Attribute-based Signature, ABS)[3]. 基于属性的签名方案保留了基于身份签名方案无需公钥证书的优点,并具有以下额外优势:首先,ABS 方案可以更有效地保护用户隐私,因此可以方便地应用于对隐私要求比较高的环境中;其次,ABS 方案的校验过程实现了基于属性的访问控制验证,为后续访问控制过程提供了便利.

自 2008 年 Maji 等[3]提出第 1 个基于属性签名方案以来,属性签名方案得到了研究者越来越多的关注,已有多个属性证明方案被提出[4-8],然而,目前的绝大多数 ABS 方案其签名长度(群元素的个数)都与策略中包含的属性线性相关,当策略中包含较多属性时,其通信效率将受到较大影响,在一定程度上阻碍了 ABS 的进一步应用.

为了解决这一问题,提高 ABS 方案的效率,Herranz 等[9]于 2012 年提出首个高效 ABS 方案的构造,在文献[9]中,Herranz 等提出 2 个 ABS 方案构造,均可实现常数个群元素的签名,其中方案 2 具有更高的效率,其签名只包含 3 个群元素,然而,该方案存在的主要问题是其私钥长度与用户属性个数和门限参数的乘积线性相关,在通常的基于属性系统中,该部分可能包含超过数千个元素,严重影响了其实用性. 而文献[9]中的方案一虽然避免了这一问题,但其签名长度大大增加(包含 15 个群元素).

本文中,我们提出一种新的门限式 ABS 方案构造,该方案可以实现常数长度的签名,与现有方案[9]相比,我们的方案避免了零知识证明方案的使用,从而具有更短的签名长度和私钥长度. 虽然文献[9]中方案二在签名长度上优于我们提出的方案,但由于其私钥长度过长,因此很难应用于储存资源受限环境.

1　预备知识

1.1　双线性映射

首先,我们将回顾双线性映射的定义,令 G, G_T 为阶为 p 的素数阶循环群, g 为群 G 的生成元. 若存在映射 $e: G \times G \rightarrow G_T$ 满足以下性质,则称 e 是从群 G 到 G_T 的一个双线性映射:

双线性:对于任意的 $g_1, g_2 \in G$, $a, b \in Z_p$, 有 $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$.

非退化性:存在 $g \in G$, 满足 $e(g,g) \neq 1$.

可计算性:对于任意的 $g_1, g_2 \in G$, 存在高效算法计算 $e(g_1, g_2)$.

1.2　安全假设

本节中,我们首先对本文提出方案使用到的安全假设进行介绍,该安全假设是对 q-SDH 安全假设的一个扩展,在附录 A 中,我们在一般群模型下给出了对该假设安全性的证明.

定义 1(安全假设 1):对于阶为 p 的素数阶循环群 G, G_T,以及双线性映射 $e: G \times G \rightarrow G_T$, 给定元组 $(g, g^z, g^{x^2}, \cdots, g^{x^q}, h)(x \in Z_p, g, h \in G)$ 以及 2 个多项式 $F(x) = \prod_{i=1}^{m}(x + c_i)$ 和 $G(x) = \prod_{j=m+1}^{2q+1}(x + c_j)$,其中 $c_1, c_2, \cdots, c_{2q+1} \in Z_q$ 且两两不等,则不存在多项式时间算法可以有效计算 4 元组 S, T, U, V 满足 $e(S,g)^{F(x)} = e(T,U), U = V^{G(x)}$.

2　定义

在本节中,我们将给出基于属性签名的定义与安全模型.

2.1　基于属性的签名方案

根据文献[3]中的定义,对于属性空间 P, 基于属性的签名(ABS)方案由 Setup、KeyGen、Sign 和 Verify 4 个多项式时间算法组成:

Setup:该算法根据输入的安全参数 1^λ 生成公共参数 *params* 与属性权威的主私钥 *MSK*.

KeyGen:根据用户属性为用户 u 颁发签名密钥,对于输入 *params*, *MSK* 和给定的属性集合 $A \subseteq P$, 输出用户私钥 sk_u.

Sign: 签名生成算法,对于输入消息 M, 访问结构 Υ, 用户私钥 sku, 如果 $\Upsilon(A) = 1$, 即用户的属性集合满足访问结构,则计算对应的签名 σ.

Verify:签名校验算法,对于给定的签名 σ 及对应的消息 M 和访问结构 Υ, 如果签名合法,则输出 *acc*, 否则输出 *rej*.

在本文中将使用门限式访问结构 $\Upsilon_{k,\omega}$, 其定义为: $\Upsilon_{k,\omega}(\omega') = 1 \leftrightarrow |\omega \cap \omega'| \geqslant k$.

2.2 安全模型

对于 ABS 方案,其主要安全性质包括不可伪造性和隐私性.

不可伪造性要求只有持有满足访问结构的私钥的用户才能生成合法的签名并通过校验. 此外,不可伪造性还要求用户无法通过组合他们拥有的私钥生成原本无法生成的签名或获得其原本不拥有的属性私钥.

对于用户隐私性,本文采用文献[3]中的定义,该定义要求校验者无法从签名中获取除用户属性满足访问结构以外的任何身份和属性信息. 即对于两个同时满足给定访问结构的签名,校验者无法区分上述签名是否是由同一个用户生成的.

不可伪造性和隐私性的具体定义如下:

2.2.1 不可伪造性

本文采用与文献[9]中方案相同的选择安全模型,该模型中,敌手可以访问以下预言机:

密钥生成预言机:给定属性集合 A, 输出对应的用户私钥 sk_u, 对该预言机的查询记为 $AttrGen(A)$.

签名预言机:给定消息 M, 访问结构 Y, 输出对应的签名 σ, 对该预言机的查询记为 $AltSign(M,Y)$.

则根据文献[9],有以下的攻击 Game:

Init: 首先,敌手 F 选择要攻击的访问结构 $Y^* = (t^*, A^*)$, $|A^*| = k$.

Setup: 挑战者 C 执行签名方案的 Setup.,记录主私钥 MSK 并将公共参数 $params$ 发送给敌手 F.

Phase1: F 可以访问密钥生成预言机和签名预言机,获取若干私钥和签名,C 记录对上述预言机的所有查询输入.

Forgery: F 给出伪造的签名 σ^*, 对应的消息为 M^*, 访问结构 Y^*.

如果 σ^* 是关于 M^* 与 Y^* 的一个合法签名,且敌手从未使用 M^*, Y^* 作为输入对签名预言机进行查询,同时对于密钥生成预言机的所有输入属性集合 A, 有 $Y^*(A) = 0$, 则称敌手 F 获得此次 Game 的胜利. 对于任一敌手 F,将其获得胜利的概率记为 $AdvF(1^\lambda)$.

定义 2(不可伪造性):如果对于一个 ABS 方案,不存在多项式时间敌手可以以不可忽略的概率获得上述不可伪造 Game 的胜利,则称该 ABS 方案对于选择访问结构敌手具有不可伪造性.

2.2.2 隐私性

对于隐私性,本文采用如下定义:

定义 3(完全隐私性[3]):对于一个 ABS 方案,若对于任意属性集合 A_1, A_2, 消息 M, 和所有满足 $Y(A_1) = Y(A_2) = 1$ 的访问结构 Y, 有 $Sign(KeyGen(MK, A_1), M, Y)$ 与 $Sign(KeyGen(MK, A_2), M, Y)$ 的输出分布相同,则称该 ABS 方案具有完全隐私性.

3 方案构造

令 G, G_T 为阶为 p 的素数阶循环群, g 为群 G 的生成元, $e: G \times G \to G_T$ 为第 1 节中定义的双线性映射,则本文提出的基于属性签名方案构造如下:

Setup: 首先,对于系统中的所有属性,为其分配属性值 $\omega_i \in Z_p^*$. 接下来,选择方案支持的最大门限值 n, 然后选择 $n-1$ 个冗余属性 $d_j \in Z_p^*$ $(j = 1, \cdots, n-1)$, 这些属性不会被颁发给任何用户. 之后,随机选择 $x, x_0 \in Z_p^*, h \in G$, 并计算 $(g, g^x, g^{x^2}, \cdots, g^{x^{2n-1}}, h, h^x, h^{x^2}, \cdots, h^{x^{n-1}}), h_0 = g^{x_0}$. 最后,选取用于消息摘要的散列函数 $H(\cdot): \{0,1\}^* \to Z_p^*$ 及 $C \in G$, 则主密钥 $MSK = x, x_0$, 系统公共参数定义为

$$params = \{G, G_T, e, (g, g^x, g^{x^2}, \cdots, g^{x^{2n-1}}, h, h^x, h^{x^2}, \cdots, h^{x^{n-1}}), h_0, \Omega = \{\omega_i\}, D = \{d_j\}, C, H()\}$$

KeyGen: 对于要颁发的用户属性集合 $A_u (A_u \cap D = \Phi)$, 首先随机选择 $g_u \in G$ 并计算 $h_u = g_u^{1/x_0}$, 之后对于 A_u 中的每个属性 ω_{U_i}, 计算 $U_i = g_u^{\frac{1}{x+\omega_{U_i}}}$, 最后,输出用户签名密钥 $sk_u = (g_u, h_u, U_i \mid \omega_{U_i} \in \Omega_u)$.

Sign: 当用户要生成关于消息 M 与门限式访问结构 $Y = (t, A)$ 的属性签名时,执行以下操作:首先,从他拥有的属性集合中选取满足访问结构的子集 Ω_u', 即 $|\Omega_u'| = t, \Omega_u' \subseteq A \cap \Omega_u$. 之后,用户选择冗余属性集合 D 中的前 $n+t-k-1$ 个元素,记这些元素组成的集合为 $D_{n+t-k-1}$, 由于 $t \leqslant k$, 因此 $n+t-k-1 \leqslant n-1$, 所以这一操作必然可以执行.

接下来用户可以使用文献[10]中的聚合算法使用 $U_i = g_u^{\frac{1}{x+\omega_{U_i}}}$ 计算 $A_1 = g_u^{\frac{1}{\prod_{\omega_{U_i} \in \Omega_u'} (x+\omega_{U_i})}}$,

由于 $|D_{n+t-k-1} \cup (A \backslash \Omega'_u)| = (n+t-k-1)+(k-t) = n-1$,因此用户可以使用公共参数计算 $A_2 = g^{P(x)}$, $A_3 = h^{P(x)}(P(x) = \prod_{\omega \in D_{n+t-k-1} \cup (A \backslash \Omega'_u)}(x+\omega))$. 最后,用户随机选择 $r_u, r_q, r_m \in Z_p^*$ 并计算:

$$\sigma_1 = A_1^{r_u r_q} \cdot (C \cdot H(M \| Y))^{r_m}, \sigma_2 = A_2^{r_q}, \sigma_3 = A_3^{r_q}, \sigma_4 = g_u^{r_u}, \sigma_5 = h_u^{r_u}, \sigma_6 = g^{r_m} \prod_{\omega \in D_{n+t-k-1} \cup A^{(x+\omega)}}$$

则最终生成的签名为 $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6)$.

Verify: 对于给定的签名 $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6)$, 校验者校验以下等式是否成立:

$$e(\sigma_1, g^{\prod_{\omega \in D_{n+t-k-1} \cup A^{(x+\omega)}}}) = e(\sigma_4, \sigma_2)\, e(C \cdot H(M \| Y), \sigma_6), e(\sigma_2, h) = e(\sigma_3, g),$$

与 $e(\sigma_4, g) = e(\sigma_5, h_0)$. 若上述等式均成立,则输出 *acc*, 否则输出 *rej*.

4　安全性分析

4.1　正确性

对于校验过程中的第二和第三校验等式,根据定义容易验证其正确性,对于第一校验等式,其正确性如下.

$$e(\sigma_1, g^{\prod_{\omega \in D_{n+t-k-1} \cup A^{(x+\omega)}}}) =$$
$$e(A_1^{r_u r_q} \cdot (C \cdot H(M \| Y))^{r_m}, g^{\prod_{\omega \in D_{n+t-k-1} \cup A^{(x+\omega)}}}) =$$
$$e(A_1^{r_u r_q}, g^{\prod_{\omega \in D_{n+t-k-1} \cup A^{(x+\omega)}}}) \cdot$$
$$e((C \cdot H(M \| Y))^{r_m}, g^{\prod_{\omega \in D_{n+t-k-1} \cup A^{(x+\omega)}}}) =$$
$$e(g_u^{\frac{r_u r_q}{\prod_{\omega_{U_i} \in \Omega_u'^{(x+\omega_{U_i})}}}}, g^{\prod_{\omega \in D_{n+t-k-1} \cup A^{(x+\omega)}}}) \cdot$$
$$e((C \cdot H(M \| Y)), g^{r_m \prod_{\omega \in D_{n+t-k-1} \cup A^{(x+\omega)}}}) =$$
$$e(g_u^{r_u r_q}, g^{\prod_{\omega \in D_{n+t-k-1} \cup (A \backslash \Omega'_u)^{(x+\omega)}}}) \cdot$$
$$e(C \cdot H(M \| Y), \sigma_6) =$$
$$e(g_u^{r_u r_q}, A_2) e(C \cdot H(M \| Y), \sigma_6) =$$
$$e(\sigma_4, \sigma_2) e(C \cdot H(M \| Y), \sigma_6).$$

4.2　隐私性

根据定义,本文所述方案的签名共包含 6 个元素,根据方案中 $\sigma_2 = A_2^{r_q}, \sigma_4 = g_u^{r_u}, \sigma_6 = g^{r_m} \prod_{\omega \in D_{n+t-k-1} \cup A^{(x+\omega)}}$ 的定义可知对于随机选取的 r_u, $r_q, r_m \in Z_p^*$, 上述元素在群 G 中均匀分布. 而由校验等式 $e(\sigma_2, h) = e(\sigma_3, g), e(\sigma_4, g) = e(\sigma_5, h_0)$ 可知 σ_3, σ_5 的值由 σ_2, σ_4 与系统参数 x_0, h 唯一确定,因此其分布与签名者身份和属性无关. 最后,根据校验等式 $e(\sigma_1, g^{\prod_{\omega \in D_{n+t-k-1} \cup A^{(x+\omega)}}}) = e(\sigma_4, \sigma_2) e(C \cdot H(M \| Y), \sigma_6)$, 可知 σ_1 的值由 $\sigma_2, \sigma_4, \sigma_6$ 与 C, M, Y 的值决定,因此对于任意属性集合 A_1, A_2, 消息 M, 和满足 $Y(A_1) = Y(A_2) = 1$ 的访问结构 Y, $Sign(KeyGen(MK, A_1), M, Y)$ 与 $Sign(KeyGen(MK, A_2), M, Y)$ 的输出分布完全相同. 综上所述,本文提出的 ABS 方案具有完全隐私性.

4.3　不可伪造性

对于不可伪造性,有如下定理:

定理 1:若定义 1 中假设成立,则本文提出的基于属性签名方案在随机预言机模型下对于选择访问结构敌手具有不可伪造性.

证明:如果任何敌手可以在选择访问结构安全模型下破坏本文所提出的基于属性签名方案的不可伪造性,则可以利用该敌手构造算法破坏定义 1 中的安全假设,. 根据定义 1,对于阶为 q 的素数阶循环群 G, G_T,以及双线性映射 $e: G \times G \rightarrow G_T$, 挑战者获取元组 $(g, g^{\gamma}, g^{\gamma^2}, \cdots, g^{\gamma^q}, h)(\gamma \in Z_p, g, h \in G)$ 以及两两不等的 $c_1, c_2, \cdots, c_{2q+1} \in Z_q$, 挑战者的目的是在多项式时间内计算四元组 S, T, U, V 满足 $e(S, g)^{F(\gamma)} = e(T, U), U = V^{G(\gamma)}$, 其中 $F(\gamma) = \prod_{i=1}^{m}(\gamma + c_i)$ 以及 $G(\gamma) = \prod_{j=m+1}^{2q+1}(\gamma + c_i)$ 为 2 个多项式. 则挑战者按照以下流程与敌手进行不可伪造 Game:

Init: 首先,敌手 F 选择要攻击的访问结构 $Y^* = (t^*, A^*), |A^*| = k$.

Setup: 挑战者首先生成属性集合,对于挑战 $(g, g^{\gamma}, g^{\gamma^2}, \cdots, g^{\gamma^q}, h)(\gamma \in Z_p, g, h \in G)$, 挑战者从 $c_1, c_2, \cdots, c_m \in Z_q$ 中随机选择属性值,分配给 A^* 中的所有属性以及冗余属性集合 D 中的前 $n + t^* - k^* - 1$ 个属性,将 $c_1, c_2, \cdots, c_m$ 未分配的值的集合记作 Y, 对于冗余属性集合 D 中的所有其他属性,挑战者从 $Zq \backslash C$ 中随机选择对应的属性值. 接下来,将 $c_{m+1}, c_{m+2}, \cdots, c_{2q+1}$ 随机分配给 $\Omega \backslash A^*$ 中的属性,并将 $c_{m+1}, c_{m+2}, \cdots, c_{2q+1}$ 中未分配出去属性的集合记为 H.

之后,挑战者令 $x = \gamma, x_0 = G(x), y = \prod_{\omega \in Y}(x+\omega), h = g^y, h_0 = g^{x_0}$ 并选取 $H(\cdot): \{0,1\}^* \rightarrow Z_p^*$ 及 $C \in G$, 至此,挑战者可以在不知道秘密值 γ 的情况下,使用 $g, g^{\gamma}, g^{\gamma^2}, \cdots, g^{\gamma^q}, h$ 计算公共参数 $params = \{G, G_T, e, (g, g^x, g^{x^2}, \cdots, g^{x^{2n-1}}, h, h^x, h^{x^2}, \cdots, h^{x^{n-1}}), h_0, \Omega = \{\omega_i\}, D =$

$\{d_j\}, C, H(\,)\}$.

Phase1：对于第 k 次密钥签发查询，设其输入为 $A = \Omega_{u_k}$，则挑战者随机选择 u_k 并设 $g_k = g^{u_k x_0} \prod_{\omega \in A \cap A^*} (x+\omega)$，之后计算 $U_{k_i} = g_k^{\frac{1}{x+\omega_{U_i}}}, h_k = g_k^{1/x_0} = g^{u_k} \prod_{\omega \in A \cap A^*} (x+\omega)$. 根据安全模型，有 $|\Omega_{u_k} \cap A| < t^*$，因此 $x_0 \prod_{\omega \in \Omega_{u_k} \cap A^*} (x+\omega) = G(x) \prod_{\omega \in \Omega_{u_k} \cap A^*} (x+\omega)$. 这一多项式的次数最高为 q，所以挑战者可以使用挑战值计算 g_k, h_k, U_{k_i}. 最后，挑战者返回 $sk_{U_k} = (g_k, h_k, U_{k_i})$.

对于签名查询，设其输入为 $M, Y = (t, A)$，则挑战者随机选择 $\eta, r_1, r_6 \in Z_p$，计算 $\sigma_1 = g^{x_0 r_1}$，$\sigma_6 = g^{x_0 r_6}$，并使用随机预言机返回 $H(M \| Y) = C^{-1} \cdot g^{\frac{r_1}{r_6} \cdot [(\prod_{\omega \in (A \cap A^*)} (x+\omega)) - \eta] (\prod_{\omega \in (A \setminus A^*) \cup D_{n+t-|A|-1}} (x+\omega))}$. 则为生成合法的签名，$\sigma_3, \sigma_4$ 的值必须满足 $e(\sigma_3, \sigma_4) = e(g,g)^{\eta r_1 x_0 y \cdot \prod_{\omega \in (A \setminus A^*) \cup D_{n+t-|A|-1}} (x+\omega)}$.

考虑如下集合：

$S = H \cup (\Omega \setminus A^*) \cup (A \setminus A^*) \cup D_{n+t-|A|-1} \cup Y = H \cup (\Omega \setminus A^*) \cup D_{n+t-|A|-1} \cup Y$. 该集合包含 $2q - t - n + 2 < 2q$ 个元素，因此可以把多项式 $L(x) = \eta r_1 G(x) \prod_{\omega \in Y} (x+\omega) \cdot \prod_{\omega \in (A \setminus A^*) \cup D_{n+t-|A|-1}} (x+\omega)$. 表示为 2 个次数均不大于 q 的多项式的乘积，其中分别包含 $x_0 = G(x)$ 与 $y = \prod_{\omega \in Y} (x+\omega)$，记 $L(x) = F_3(x) F_4(x) = [yF_2(x)][x_0 F_5(x)]$，则挑战者计算 $\sigma_2 = g^{F_2(x)}, \sigma_3 = g^{F_3(x)}, \sigma_4 = g^{F_4(x)}, \sigma_5 = g^{F_5(x)}$ 并输出签名 $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6)$.

对于第 j 次随机预言机查询，如果输入中不包含挑战结构 Y^*，则挑战者令 $H(M \| Y) = C^{-1} \cdot g^{\frac{r_{1j}}{r_{6j}} \cdot [(\prod_{\omega \in (A \cap A^*)} (x+\omega)) - \eta] (\prod_{\omega \in (A \setminus A^*) \cup D_{n+t-|A|-1}} (x+\omega))}$，以模拟签名查询. 否则挑战者猜测该次查询是否会应用于最终的伪造签名中，如果是，则挑战者随机选择 r_h，返回 $H(M \| Y^*) = g^{r_h} \prod_{\omega \in A^* \cup D_{n+t-|A^*|-1}} (x+\omega)$，并记录此次查询对应的消息 M，对于其他查询，返回 $H(M \| Y^*) = C^{-1} \cdot g^{\frac{r_{1j}}{r_{6j}} \cdot [(\prod_{\omega \in (A \cap A^*)} (x+\omega)) - \eta] (\prod_{\omega \in (A \setminus A^*) \cup D_{n+t-|A|-1}} (x+\omega))}$.

Forgery：最终，敌手输出一个伪造签名 $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*, \sigma_5^*, \sigma_6^*)$，如果该签名对应的消息与猜测不一致，则挑战者中止并输出 $\perp$，对于最多包含 N 次随机预言机查询的 Game，可知挑战者不中止的概率至少为 $1/N$，在这种情况下，根据安全模型，有

$e(\sigma_1^*, g^{\prod_{\omega \in D_{n+t-k-1} \cup A^*} (x+\omega)}) = e(\sigma_2^*, \sigma_4^*) e(C \cdot H(M \| Y), \sigma_6^*), \sigma_4^* = \sigma_5^{* x_0}$.

由 $H(M \| Y^*) = g^{r_h} \prod_{\omega \in A^* \cup D_{n+t-|A^*|-1}} (x+\omega)$，挑战者可以计算 $\sigma_0^* = (\sigma_1^* / \sigma_6^*)^{r_h}$ 满足

$e(\sigma_0^*, g^{y \prod_{\omega \in D_{n+t-k-1} \cup A^*} (x+\omega)}) = e(\sigma_3^*, \sigma_4^*)$

由于 $x_0 = G(x), y \cdot \prod_{\omega \in A^* \cup D_{n+t-|A|-1}} (x+\omega) = F(x)$，可知四元组 $(\sigma_0^*, \sigma_3^*, \sigma_4^*, \sigma_5^*)$ 是对于挑战问题的一个解，至此挑战者使用敌手构造出了解决安全问题 1 的算法.

综上所述，在假设定义 1 中安全假设成立的情况下，本文提出的 ABS 方案具有不可伪造性，定理得证.

5 效率分析

在本章中，我们将从签名长度和私钥长度方面对比本文方案与现有常数签名长度的门限式 ABS 方案的效率，表 1 给出对比结果，其中 n 为系统支持的最大门限值，k 为用户拥有的属性个数.

表 1 方案效率比较

Table 1 Efficiency comparison

	签名长度（群元素个数）	私钥长度（群元素个数）
本文方案	6	$k+2$
文献[9]方案 1	15	$k+n$
文献[9]方案 2	3	$(2n+2)(k+n)$

由表 1 可见，文献[9]中方案 2 具有最短的签名长度，但是其私钥长度与系统最大门限值和用户属性个数的乘积线性相关，以常见的基于属性系统为例，典型的取值为 $n = 20, k = 80$，此时该方案的私钥长度为 4 200 个群元素，严重影响了其实用性.

对于文献[9]中方案 1，其私钥长度较之方案 2 大大降低，但由于本文避免使用关于双线性映射的零知识证明方案，因此签名长度与之相比缩短 60%. 同时，本文方案在私钥长度和计算代价方面都比该方案具有更高的效率.

6 结语

本文提出一种新的门限式基于属性签名的构

造方法,可以实现与访问结构无关的常数长度签名.与现有常数长度基于属性签名相比,本文方案在保持私钥长度可接受的条件下,缩短了签名长度和私钥规模.

接下来,本文在随机预言机模型下对本文提出的签名方案进行了安全性证明,在下一步工作中我们将在保持该方案效率的情况下,寻找可以在标准模型下证明方案安全性的方法.

参考文献

[1] Sahai A, Waters B. Fuzzy Identity-based encryption[C]// Eurocrypt 2005, LNCS 3494. Springer-Verlag, 2005: 457-473.

[2] Shamir A. Identity-based cryptosystems and signature schemes[C]// Crypto 84, LNCS 196. Springer-Verlag, 1984:47-53.

[3] Maji H, Prabhakaran M, Rosulek M. Attribute based signatures: achieving attribute privacy and collusion-resistance[C/OL]// (2008)[2014-07-20]. http://eprint.iacr.org/2008/328.

[4] Li J, Au M H, Susilo W, et al. Attribute-based signature and its applications[C]// ASIACCS'10, ACM. 2010: 60-69.

[5] Li J, Kim K. Attribute-based ring signatures[C/OL]// (2008)[2014-07-20]. http://eprint.iacr.org/2008/394.

[6] Escala A, Herranz J, Morillo P. Revocable attribute-based signatures with adaptive security in the standard model[C]// AFIRICACRYPT 2011, LNCS 6737. Springer-Verlag, Berlin, 2011:224-241.

[7] Maji H, Prabhakaran M, Rosulek M. Attribute-based signatures[C]// CT-RSA 2011, LNCS6558. Springer-Verlag, 2011:376-392.

[8] Shahandashti S F, Safavi-Naini R. Threshold attribute-based signatures and their application to anonymous credential systems[C]// AricaCrypt'09, LNCS5580. Springer-Verlag, 2009:198-216.

[9] Herranz J, Laguillaumie F, Libert B, et al. Short attribute-based signatures for threshold predicates[C]// CT-RSA 2012, LNCS7178. Springer-Verlag, 2012:51-67.

[10] Delerablbee C, Pointcheval D. Dynamic threshold public-key encryption[C]// Crypto 2008, LNCS 5157. Springer-Verlag, 2008:317-334.

[11] Shoup V. Lower bounds for discrete logarithms and related problems[C]// Eurocrypt 1997, LNCS 1233. Springer-Verlag, 1997:256-266.

附录 A　安全假设的安全性分析

在本文中,我们提出一个新的计算性安全假设,在本章中,我们将使用一般群模型[11]分析该假设的困难性.

在一般群模型下,所有群元素由模拟器生成,模拟器记录这些元素的离散对数值.此外,模拟器将每个群元素与某些有理函数相关联,在敌手查询群元素时返回该函数的特定编码值,具体规则如下:

1:对应于群元素 g.

$x,x^2,\cdots,x^q$:对应于群元素 $g^x,g^{x^2},\cdots,g^{x^q}$.

当敌手通过编码值询问对于值 α 和 β 进行群运算的结果时,模拟器返回函数 $F_\alpha + F_\beta$ 的编码值.

当敌手通过编码值询问对于值 α 进行 d 次指数运算的结果时,模拟器返回函数 $d \cdot F_\alpha$ 的编码值.

由于有理函数的变量是在群 Z_p 中随机选择的,因此当 2 个函数的表达式不一致时,对应的群元素相同的概率可以忽略.

对于定义 1 中的安全问题,最终敌手输出四元组 S,T,U,V, 满足等式 $e(S,g)^{F(x)} = e(T,U), U = V^{G(x)}$. 记 S,T,U,V 对应的离散对数值为 s,t,u,v, 根据一般群假设, s,t,u,v 只能由初始群元素经过一般群操作生成,因此其必然具有如下形式:

$$s = s_0 + s_1 x + \cdots + s_q x^q,$$

$$t = t_0 + t_1 x + \cdots + t_q x^q,$$

$$u = u_0 + u_1 x + \cdots + u_q x^q,$$

$$v = v_0 + v_1 x + \cdots + v_q x^q.$$

由等式 $e(S,g)^{F(x)} = e(T,U), U = V^{G(x)}$, 可知 $sF(x) = tu, u = vG(x)$, 由于 s,t,u,v 皆为关于 x 的多项式,且根据假设 $F(x)$ 与 $G(x)$ 间不存在公因式,因此必然存在多项式 $\tilde{s}$ 使得 $s = \tilde{s}G(x)$, 则有 $\tilde{s}F(x) = tv$, 再根据 $u = vG(x)$, 可知多项式 v 的次数不大于 $m - q - 1$, 即 tv 的次数不大于 $m - 1$, 相对的, $\tilde{s}F(x)$ 的次数不低于 m, 因此 2 式不可能相等.

综上所述,定义 1 中所述安全问题在一般群模型下是难解的,故安全假设成立.