一种标准模型下基于身份的有效门限环签名方案*

孙 华[1], 郭 磊[1], 郑雪峰[2], 王爱民[1]
(1. 安阳师范学院 计算机与信息工程学院, 河南 安阳 455000; 2. 北京科技大学 计算机与通信工程学院, 北京 100083)

摘 要: 在门限环签名中,任意 n 个成员组中的 t 个成员可以代表整个成员组产生 (t,n) 门限环签名,而对实际的签名者却具有匿名性。为了设计基于身份的门限环签名方案,利用双线性对技术,提出了一种在标准模型下基于身份的有效门限环签名方案,并对方案的安全性进行了分析。最后证明了方案满足无条件匿名性,以及在 CDH 困难问题的假设下满足适应性选择消息和身份攻击下的存在不可伪造性。

关键词: 基于身份的密码学; 门限环签名; 双线性对; CDH 问题
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2012)06-2258-04
doi:10.3969/j.issn.1001-3695.2012.06.068

Efficient identity-based threshold ring signature in standard model

SUN Hua[1], GUO Lei[1], ZHENG Xue-feng[2], WANG Ai-min[1]
(1. *School of Computer & Information Engineering, Anyang Normal University, Anyang Henan* 455000, *China*; 2. *School of Computer & Communication Engineering, University of Science & Technology Beijing, Beijing* 100083, *China*)

Abstract: The (t,n) threshold ring signature could be generated by any t entites of n entities group on behalf of the whole group, while the actual signers remain anonymous. In order to design an identity-based threshold ring signature, this paper presented an efficient identity-based threshold ring signature scheme in the standard model and gave its security analysis in terms of bilinear pairing technique. In the last, it proved this scheme satisfied the unconditional signer ambiguity and existential unforgeability against adaptive chosen message and identity attacks in terms of the hardness of CDH problem.

Key words: identity based cryptography; threshold ring signature; bilinear pairing; computational Diffie-Hellman problem

1984 年,Shamir[1] 首先提出了基于身份的公钥密码体制,用于解决传统公钥密码体制中的证书管理问题。在基于身份的密码体制中,用户的公钥为能够标志用户身份的信息,如 e-mail地址或 IP 地址,而其私钥则由可信第三方生成。2001 年,Boneh 等人[2] 利用双线性对技术提出了第一个实用的基于身份的加密方案,随后人们又提出了一些基于身份的签名方案[3,4]。匿名性是密码学应用中的一个重要属性。在实际的应用中,如电子现金和电子选举中,需要确保签名者的信息不被泄露。环签名[5] 首先由 Rivest 等人提出,它由某一用户代表某一群用户产生,验证者可以对它进行验证却不知道谁是真正的签名者,因此,环签名可以实现签名者的匿名性。随后许多环签名方案[6~8] 被相继提出。不同于群签名[9,10],环签名中群的形成是自发的,不需要有群管理者,签名者只需要选取群成员的公钥和自己的私钥,就可以生成环签名。这种签名方案可以极大地降低相互认证的复杂性,同时又能够提供签名者的匿名性。2002 年,Bresson 等人[11] 提出了一个在随机模型下的门限环签名方案,随后人们又陆续提出了一些具有不同性质的门限环签名方案[12~14]。Sherman 等人[15] 提出了第一个在随机模型下基于身份的门限环签名方案。

可证明安全性理论是在一定的安全模型下用归约的方法证明所提出的方案能够达到特定的安全目标。目前,已有的门限环签名方案大多是在随机预言模型下进行安全性证明的。然而,在随机预言模型中,把 hash 函数看做一个完全随机的理想模型是一个很强的要求,在具体应用中有时却无法构造相应的实例。因此,设计在标准模型下高效可证安全的门限环签名方案更有实际意义。

本文提出了一种基于身份的门限环签名方案,并给出了相应的安全模型,同时,利用 CDH 问题的困难性证明了方案存在不可伪造性。因此,本文方案是安全可靠的。

1 预备知识

1.1 双线性对

设 G、G_T 是两个阶为素数 p 的循环加法群和循环乘法群,g 是群 G 的生成元,双线性对 $e:G\times G\to G_T$ 是具有如下性质的映射:

a)双线性。对于所有的 $P,Q\in G$ 与 $a,b\in Z_p^*$,都有 $e(aP,bQ)=e(P,Q)^{ab}$。

b)非退化性。$e(g,g)\neq 1$。

c)可计算性。存在一个有效的算法计算 $e(P,Q)$,其中,$P,Q\in G$。

1.2 困难问题假设

DLP 问题:已知 P 是群 G 的生成元,给定任意的 $Q\in G$,求满足方程 $xP=Q$ 的解 x。

CDH 问题:已知 G 是阶为素数 p 的循环群,g 是群 G 的生成元,给定 $g,g^a,g^b\in G,a,b\in_R Z_P^*$,计算 g^{ab}。

收稿日期: 2011-11-21; **修回日期**: 2011-12-26 **基金项目**: 国家自然科学基金资助项目(61170244);河南省科技厅科技攻关计划项目(112102210370);河南省教育厅科学技术研究重点项目(12A520002)

作者简介:孙华(1980-),男,河南安阳人,讲师,博士,主要研究方向为密码学、信息安全(sh1227@163.com);郭磊(1976-),男,讲师,硕士,主要研究方向为信息安全理论与技术;郑雪峰(1951-),男,教授,主要研究方向为网络与信息安全;王爱民(1957-),男,教授,主要研究方向为可信计算、数据挖掘.

2　基于身份的门限环签名

2.1　形式化定义

定义 1　设 $L=\{\mathrm{ID}_1,\cdots,\mathrm{ID}_n\}$ 为门限环签名中 n 个成员的集合,门限值为 t,消息为 m,基于身份(t,n)的门限环签名方案可由四个算法组成,即系统建立、私钥提取、签名和验证。

a)系统建立。给定安全参数 k,该算法生成系统参数 params 以及相应的主密钥 s。系统参数 params 是公开的,而主密钥 s 是保密的。

b)私钥提取。输入系统参数 params、主密钥 s 和用户身份 ID,该算法输出身份 ID 的私钥 s_{ID}。

c)签名。首先,各签名者 $\mathrm{ID}_i(i=1,\cdots,t)$随机选择其子秘密 s_i 以及 $t-1$ 次多项式 $f_i(x)$,广播公开参数;然后计算其他各签名者 $\mathrm{ID}_j(j\neq i)$的秘密分享,并将它们发送给其他签名者。签名者 ID_i 可以通过验证鉴别其收到的秘密分享是否正确,并最终计算其私有秘密 x_i。其次,输入身份列表 $L=\{\mathrm{ID}_1,\cdots,\mathrm{ID}_n\}$、门限值 t、消息 m 以及 t 个签名者的私钥$\{S_{\mathrm{ID}_i}\}_{i=1,\cdots,t}$,该算法输出在消息 m 下的(t,n)门限环签名 σ。

d)验证。输入门限环签名 σ、门限值 t、身份列表 $L=\{\mathrm{ID}_1,\cdots,\mathrm{ID}_n\}$。如果 σ 是由 L 中 t 个成员产生的有效门限环签名,则输出 True;否则,输出 False。

2.2　基于身份门限环签名(IBTRS)的安全模型

下面介绍基于身份门限环签名的安全模型,包括不可伪造性和匿名性。

定义 2　一个基于身份的门限环签名在适应性选择消息和身份攻击下满足密文的存在不可伪造性,如果没有概率多项式时间的敌手 A 在下面的游戏中获得不可忽略的优势:

Setup:挑战者 C 运行系统建立算法,生成系统参数并发送给敌手 A,保存主密钥 msk。

Query:敌手 A 可以适应性地向挑战者 C 发出如下询问:

Extract query:敌手 A 选择身份 ID,C 计算其私钥 s_{ID},并将其发送给 A。

Signature query:敌手 A 选择成员列表 $L=\{\mathrm{ID}_1,\cdots,\mathrm{ID}_n\}$、门限值 t 及消息 m。C 首先运行私钥提取算法产生实际签名者的私钥 s_{ID},然后运行签名算法生成(t,n)门限环签名并将其发送给 A。

Forgery:敌手 A 输出在身份列表 $L^*=\{\mathrm{ID}_1^*,\cdots,\mathrm{ID}_n^*\}$、门限值 t 和消息 m^* 下的伪造门限环签名 σ^*。这里的限制条件是至多询问了 L^* 中 $t-1$ 个身份的私钥以及(L^*,m^*)没有出现在前面的签名询问中。如果对 σ^* 的验证结果不为 False,那么 A 赢得游戏。敌手 A 的优势定义为其赢得游戏的概率,即

$$\mathrm{Adv}_A=P[A\ \text{succeeds}]$$

定义 3　如果已知任意包含 n 个成员身份的列表 $L=\{\mathrm{ID}_1,\cdots,\mathrm{ID}_n\}$对任意消息 m 的门限值为 t 的(t,n)门限环签名 σ,任何敌手能够识别实际签名者的优势不会大于随机猜测,即敌手输出实际签名者的概率不会大于 t/n,则称一个 IBTRS 方案具有无条件匿名性。

3　标准模型下基于身份的门限环签名方案

3.1　方案描述

令 G、G_T 是阶为素数 p 的循环群,$e:G\times G\to G_T$ 是一个双线性映射。两个无碰撞的哈希函数 $H_u:\{0,1\}^*\to\{0,1\}^{n_u}$和 $H_m:\{0,1\}^*\to\{0,1\}^{n_m}$将任意长度的身份 ID 和消息 m 分别输出长度为 n_u 和 n_m 的位串。方案由如下算法构成。

1)系统建立　PKG 随机选取 $\alpha\in Z_p$,生成元 $g\in G$,计算 $g_1=g^{\alpha}$。随机选取 $g_2,u',m'\in G,n_u$ 维向量 $\hat{U}=(u_i)$,n_m维向量 $\hat{M}=(m_i)$,其中 $u_i,m_i\in_R G$,则系统参数为 $\mathrm{param}=(G,G_T,e,g,g_1,g_2,u',\hat{U},m',\hat{M},H_u,H_m)$,主密钥为 $msk=g_2^{\alpha}$。

2)私钥提取　给定用户身份 ID,令 $u=H_u(\mathrm{ID})$为身份 ID 的长度为 n_u 的位串,$u[i]$表示该位串中的第 i 位,$\Phi_u\subseteq\{1,2,\cdots,n_u\}$为 $u[i]=1$ 的序号 i 的集合,PKG 任选 $r_u\in Z_p$,则身份 ID 的私钥为

$$d_{\mathrm{ID}}=(d_1,d_2)=(g_2^{\alpha}(u'\prod_{i\in\Phi_u}u_i)^{r_u},g^{r_u})$$

3)签名　设 $L=\{\mathrm{ID}_1,\cdots,\mathrm{ID}_n\}$为门限环签名中 n 个成员的集合,不妨设实际参与签名的 t 个签名者的身份下标为$\{1,2,\cdots,t\}$,未参与签名的 $n-t$ 个签名者的身份下标为$\{t+1,t+2,\cdots,n\}$。实际的签名者通过执行下面的步骤来生成基于身份的门限环签名:

a)每个签名者 ID_i 随机选取 $s_i\in Z_p$ 为其子秘密,构造系数在 Z_p、次数为 $t-1$ 的多项式 $f_i(x)$:

$$f_i(x)=a_{i,0}+a_{i,1}x+\cdots+a_{i,t-1}x^{t-1}$$

令 $s_i=a_{i,0}$,ID_i 计算 $C_{i,d}=g^{a_{i,d}}(d=0,1,\cdots,t-1)$,并向其他签名者广播,计算分享 $s_{i,j}=f_i(j)$,然后把它们发送给其他成员 $\mathrm{ID}_j(j=1,2,\cdots,t;j\neq i)$,自己保留 $s_{i,i}=f_i(i)$。

b)签名者 ID_j 从 ID_i 那里得到分享 $s_{i,j}$后,用如下等式验证其有效性:$g^{s_{i,j}}=\prod_{d=0}^{t-1}(c_{i,d})^{j^d}$,如果没有通过验证,则 ID_j 发出对 ID_i 的控告。

c)每个签名者 ID_i 计算其私有秘密为 $x_i=\sum_{j=1}^{t}s_{j,i}$。

d)对于 $i\in\{1,2,\cdots,t\}$,每个签名者 ID_i 的私钥为$(d_{i,1},d_{i,2})$,计算 $M=H_m(L,m,t)$。令 $M\subseteq\{1,2,\cdots,n_m\}$为消息 m 的位串中 $M[l]=1$ 的序号 l 的集合,计算

$$\sigma_i=(d_{i,1}(m'\prod_{k\in M}m_k)^{x_i\eta_i},d_{i,2},g^{x_i\eta_i})=$$

$$(g_2^{\alpha}(u'\prod_{k\in\Phi_{\mathrm{ID}_i}}u_k)^{r_{\mathrm{ID}_i}}(m'\prod_{l\in M}m_l)^{x_i\eta_i},g^{r_{\mathrm{ID}_i}},g^{x_i\eta_i})=(\sigma_{i1},\sigma_{i2},\sigma_{i3})$$

其中,$\eta_i=\prod_{j=1,j\neq i}^{t}\frac{j}{j-i}\bmod p$ 为拉格朗日系数。

e)t 个签名者中的任一签名者,随机选取 $r_1,\cdots,r_n\in Z_p$,计算 $U_i=u'\prod_{j\in\Phi_{\mathrm{ID}_i}}u_j$,其中 $i=1,2,\cdots,n$,以及 $\sigma=(\prod_{i=1}^{t}\sigma_{i1}(\prod_{i=1}^{n}(U_i)^{r_i}),\sigma_{12}g^{r_1},\cdots,\sigma_{t2}g^{r_t},g^{r_{t+1}},\cdots,g^{r_n},\prod_{i=1}^{t}\sigma_{i3},\sum_{i=1}^{t}f_i(x))$。

f)输出对于消息 m 和成员集合 L 的 t-门限环签名为 $\sigma=(V,R_1,\cdots,R_n,R_m,f)$。

4)验证　签名验证者可按照如下步骤来验证对于消息 m 的签名。$\sigma=(V,R_1,\cdots,R_n,R_m,f)$是否由成员集合 L 中至少 t 个签名者生成的:

a)检验多项式 f 的次数是否为 $t-1$,并且计算等式 $R_m=g^{f(0)}$是否成立。若是,则进行下面计算;否则,验证失败。

b)当且仅当等式 $e(V,g)=e(g_1,g_2)^te(U_1,R_1)\cdots e(U_n,R_n)e(m'\prod_{l\in M}m_l,R_m)$成立时,$\sigma$ 是一个有效的门限环签名。

3.2 方案正确性

方案的正确性很容易由下面的等式得到验证：

a)根据秘密共享技术，有 $\sum_{i=1}^{t} x_i\eta_i = f(0) = \sum_{i=1}^{t} f_i(0) = \sum_{i=1}^{t} s_i$，因此，$R_m = \prod_{i=1}^{t}\sigma_{i3} = g_i^{\sum_{i=1}^{t} x_i\eta_i} = g^{f(0)}$。

b)对 σ 进行验证可得

$$e(V,g) = e(\prod_{i=1}^{t}\sigma_{i1}(\prod_{i=1}^{t}(U_i)^{r_i}),g) = e(g,g_2^{ta})\cdot$$

$$e((U_1)^{r\mathrm{ID}_1+r_1}\cdots(U_t)^{r\mathrm{ID}_t+r_t}(U_{t+1})^{r_{t+1}}\cdots(U_n)^{r_n}(m'\prod_{l\in M}m_l)^{\sum_{i=1}^{t} x_i\eta_i},g) =$$

$$e(g_1,g_2)^t e(U_1,g)^{r\mathrm{ID}_1+r_1}\cdots e(U_n,g)^{r_n} e((m'\prod_{l\in M}m_l),g)^{\sum_{i=1}^{t} x_i\eta_i} =$$

$$e(g_1,g_2)^t e(U_1,R_1)\cdots e(U_n,R_n) e(m'\prod_{l\in M}m_l,R_m)$$

3.3 方案安全性

下面证明方案满足自适应选择身份和消息攻击下的存在不可伪造性和无条件匿名性。

定理 1 在 CDH 困难问题的假设下，本文的方案满足自适应选择身份和选择消息攻击下的存在不可伪造性。

证明 假设伪造者 A 能以不可忽略的优势攻击上面的方案，则能够构造算法 B，B 可以利用 A 解决 CDH 问题。

给定 B 一个 CDH 问题的实例 (g,g^a,g^b)，为了利用 A 解决该 CDH 问题，从而计算出 g^{ab}，B 模仿 A 的挑战者，过程如下：

1)系统初始化。B 设定 $l_u = 2(q_e + q_s)$、$l_m = 2q_s$，其中 q_e 是 A 私钥询问的次数，q_s 是 A 签密询问的次数。随机选择 k_u 和 k_m，满足 $0\leqslant k_u \leqslant n_u$ 和 $0\leqslant k_m \leqslant n_m$，并假定 $l_u(n_u+1) < p$ 和 $l_m(n_m+1) < p$。B 选择 $x' \in {}_RZ_{l_u}$ 及长度为 n_u 的向量 $\boldsymbol{X} = (x_i)$，其中 $x_i \in {}_RZ_{l_u}$；选择 $z' \in {}_RZ_{l_m}$ 及长度为 n_m 的向量 $\boldsymbol{Z} = (z_k)$，其中 $z_k \in {}_RZ_{l_m}$。最后 B 选择 y'、$w' \in {}_RZ_p$，长度为 n_u 的向量 $\boldsymbol{Y} = (y_i)$，长度为 n_m 的向量 $\boldsymbol{W} = (w_i)$，其中 y_i、$w_i \in {}_RZ_p$。

对于 L 中的成员身份 ID 和消息 m 的位串 $u = H_u(\mathrm{ID})$ 和 $M = H_m(L,m,t)$，本文定义以下几个函数：

$$F(\mathrm{ID}) = x' + \sum_{i\in\Phi} x_i - l_u k_u, J(\mathrm{ID}) = y' + \sum_{i\in\Phi} y_i$$

$$K(M) = z' + \sum_{i\in M} z_i - l_m k_m, L(M) = w' + \sum_{i\in M} w_i$$

算法 B 构造上面方案中的公开参数如下：

$$g_1 = g^a, g_2 = g^b$$

$$u' = g_2^{-l_u k_u + x'} g^{y'}, u_i = g_2^{x_i} g^{y_i} \quad 1\leqslant i\leqslant n_u$$

$$m' = g_2^{-l_m k_m + z'} g^{w'}, m_i = g_2^{z_i} g^{w_i} \quad 1\leqslant i\leqslant n_m$$

可以看出，这些参数的分布与一个真正的挑战者产生的公开参数的分布是一样的。这样主密钥为 $g_2^a = g^{ab}$，同时有下面的等式：

$$u'\prod_{i\in\Phi_u} u_i = g_2^{F(\mathrm{ID})} g^{J(\mathrm{ID})}, m'\prod_{i\in M} m_k = g_2^{K(m)} g^{L(m)}$$

然后算法 B 将公开参数发送给敌手 A。

2)询问 当敌手 A 发起如下询问时，算法 B 进行如下响应：

a)私钥询问。当敌手 A 询问身份 ID_u 的私钥时，虽然算法 B 不知道主密钥，但假定 $F(\mathrm{ID}_u) \neq 0 \bmod p$，B 也能够构造其私钥 d_{ID_u}。B 任选 $r_u \in Z_p$ 并计算

$$d_{\mathrm{ID}_u} = (d_{u1}, d_{u2}) = (g_1^{-\frac{J(\mathrm{ID})}{F(\mathrm{ID})}}(u'\prod_{i\in\Phi_u} u_i)^{r_u}, g_1^{-\frac{1}{F(\mathrm{ID})}} g^{r_u})$$

令 $\tilde{r}_u = r_u - a/F(\mathrm{ID})$，可以验证 d_{ID_u} 是 ID_u 的有效私钥。

$$d_{u1} = g_1^{-J(\mathrm{ID})/F(\mathrm{ID})}(u'\prod_{i\in\Phi_u} u_i)^{r_u} =$$

$$g_2^a (g_2^{F(\mathrm{ID})} g^{J(\mathrm{ID})})^{-a/F(\mathrm{ID})} (g_2^{F(\mathrm{ID})} g^{J(\mathrm{ID})})^{r_u} =$$

$$g_2^a (g_2^{F(\mathrm{ID})} g^{J(\mathrm{ID})})^{r_u - a/F(\mathrm{ID})} = g_2^a (u'\prod_{i\in\Phi_u} u_i)^{\tilde{r}_u}$$

$$d_{u2} = g_1^{-1/F(\mathrm{ID})} g^{r_u} = g^{r_u - a/F(\mathrm{ID})} = g^{\tilde{r}_u}$$

对于敌手 A 而言，算法 B 所生成的私钥与真实挑战者所生成的私钥是一致的。如果 $F(u) = 0 \bmod p$，上面的计算将无法进行，B 将失败退出。

b)签名询问。当敌手 A 询问身份列表为 $L = \{\mathrm{ID}_1,\cdots,\mathrm{ID}_n\}$、门限值为 $t(t<n)$ 以及消息为 m 的门限环签名时，算法 B 首先计算 $M = H_m(L,m,t)$，然后按照如下步骤输出 (t,n) 门限环签名：

(a)算法 B 随机选择 $s, a_0, a_1, \cdots, a_{t-1} \in Z_p$，构造次数为 $t-1$ 的多项式 $f(x) = a_0 + a_1 x + \cdots + a_{t-1}x^{t-1}$，其中 $s = a_0$。

(b)假定 L 中至少有 t 个 ID_i，$i \in (1,\cdots,n)$，满足 $F(\mathrm{ID}_i) \neq 0 \bmod p$。令 γ 为 $F(\mathrm{ID}_i) \neq 0 \bmod p$ 的 i 的集合，为方便起见，不妨设 $\gamma = (1,\cdots,t)$。算法 B 按照私钥询问中的方法构造其私钥，计算签名者 $\mathrm{ID}_i = (1,\cdots,t)$ 的私有秘密 $x_i = f(i)$，然后利用签名算法生成在 L、门限值 t 和消息 m 下的门限环签名。

如果 L 中满足条件 $F(\mathrm{ID}_i) \neq 0 \bmod p$ 的 ID_i 少于 t 个，$i \in (1,\cdots,n)$，算法 B 也可以像在私钥询问中构造私钥那样构造一个门限环签名。假定 $K(M) \neq 0 \bmod p$，则 B 随机选择 $r_1,\cdots,r_n, r_m \in Z_p$，计算

$$\sigma = ((\prod_{i=1}^{n}(U_i)^{r_i}) g_1^{\frac{-tL(M)}{K(M)}} (m'\prod_{k\in M} m_k)^{r_m}, g^{r_1},\cdots,g^{r_n}, g_1^{\frac{-t}{K(M)}} g^{\bar{r}_m}, f(x)) =$$

$$(g_2^{ta}(\prod_{i=1}^{n}(U_i)^{r_i})(m'\prod_{k\in M} m_k)^{\bar{r}_m}, g^{r_1},\cdots,g^{r_n}, g^{\bar{r}_m}, f(x))$$

其中：$\bar{r}_m = r_m - ta/K(M)$。可见 σ 是一个有效的门限环签名。如果 $K(M) = 0 \bmod p$，上面的计算将无法进行，B 将失败退出。

3)伪造 敌手 A 输出在身份列表 $L^* = \{\mathrm{ID}_1^*,\cdots,\mathrm{ID}_n^*\}$、门限值 t 和消息 m^* 下的伪造门限环签名 σ^*。如果在整个过程中算法 B 没有失败退出，那么算法 B 检查下列条件是否成立：

a)$F(\mathrm{ID}_i^*) = 0 \bmod p$ 对于所有的 $i \in (1,\cdots,n)$ 都成立；

b)$K(M^*) = 0 \bmod p$，其中 $M^* = H_m(L,m^*,t)$。

如果上述条件不同时成立，那么算法 B 将失败退出；否则，B 可计算

$$\left(\frac{V}{R_1^{J(\mathrm{ID}_1^*)}\cdots R_n^{J(\mathrm{ID}_n^*)} R_m^{L(M^*)}}\right)^{1/t} =$$

$$\left(\frac{g_2^{ta}(u'\prod_{i\in\Phi_1} u_i)^{r_1}\cdots(u'\prod_{i\in\Phi_n} u_i)^{r_1}(m'\prod_{k\in M} m_j)^{r_m}}{g^{J(\mathrm{ID}_1^*)r_1}\cdots g^{J(\mathrm{ID}_n^*)r_n} g^{L(M^*)r_m}}\right)^{1/t} =$$

$$(g_2^{ta})^{1/t} = g_2^a = g^{ab}$$

这就是 CDH 问题的解。

因此，如果存在一个敌手可以不可忽略的概率伪造一个有效的门限环签名，那么就存在一个算法可以不可忽略的概率解决 CDH 问题，而这与 CDH 问题是一个困难问题相矛盾，故方案满足自适应选择消息和身份攻击下的存在不可伪造性。

定理 2 本文所提出的基于身份的门限环签名方案满足无条件匿名性。

证明 方案门限环签名 σ 中的多项式 $f(x) = \sum_{i=1}^{t} f_i(x)$ 是由 t 个签名者随机选择而得到的，因此，签名者的私有秘密 x_i 是随机分布的。另外，σ 中 $R_{t+1},\cdots,R_n,R_m$ 是随机生成的，没有

提供实际签名者的任何信息。对于 $R_i(i=1,\cdots,t)$ 而言,$R_i = g^{r_i + r_{\mathrm{ID}_i}}$,其中 r_{ID_i} 是由私钥生成中心(与实际签名人独立)随机选择的,r_i 是由签名者随机选择的,因此 $R_i(i=1,\cdots,t)$ 的分布是随机的。考虑 $V = g_2^{ta}(U_1)^{r_{\mathrm{ID}_1}+r_1}\cdots(U_t)^{r_{\mathrm{ID}_t}+r_t}(U_{t+1})^{r_{t+1}}\cdots(U_n)^{r_n}(m'\prod_{i\in M}m_i)^{f(0)}$,其中 g_2^a 是主密钥,指数部分 $r_1 + r_{\mathrm{ID}_1},\cdots, r_t + r_{\mathrm{ID}_t}, r_{t+1},\cdots,r_n, f(0)$ 都是随机的,因而无法提供有关实际签名人的任何信息。综上所述,即使敌手获得身份列表中所有成员的私钥,他也无法以不可忽略的优势猜测出实际签名者的身份,故本文的门限环签名方案是无条件匿名的。

4　结束语

门限环签名是一种重要的具有特殊性质的签名形式,现有基于身份的门限环签名方案的安全性大多是在随机模型下证明的。本文在标准模型下设计了一个基于身份的(t,n)门限环签名方案,通过对方案的安全性进行证明,指出方案在 CDH 困难问题的假设下满足自适应选择消息和身份攻击下的存在不可伪造性,因此,本文所提出的方案是安全的。

参考文献:

[1] SHAMIR A. Identity-based cryptosystems and signature schemes [C]//Proc of CRYPTO'84 on Advances in Cryptology. New York: Springer-Verlag,1984:47-53.

[2] BONEH D,FRANKLIN M. Identity-based encryption from the weil pairing[C]//Proc of the 21st Annual International Cryptology Conference on Advances Cryptology. Berlin:Springer-Verlag,2001:213-229.

[3] HESS F. Efficient identity based signature schemes based on pairings [C]//Proc of SAC. Berlin:Springer-Verlag,2002:310-324.

[4] PATERSON K G,SCHULDT J C N. Efficient identity-based signatures secure in the standard model [C]//Proc of ACISP. Berlin: Springer-Verlag,2006:207-222.

[5] RIVEST R L,SHAMIR A,TAUMANY. How to leak a secret[C]// Proc of ASIACRYPT. Berlin:Springer-Verlag,2001:552-565.

[6] WANG Hua-qun, ZHANG Fu-tai, SUN Yan-fei. Cryptanalysis of a generalized ring signature scheme[J]. IEEE Trans on Dependable and Secure Computing,2009,6(2):149-151 .

[7] WANG Hua-qun, ZHAO Shu-ping. Cryptanalysis of several linkable ring signature schemes[C]//Proc of NSWCTC. [S.l.]:IEEE Press, 2010:302-305.

[8] HU Cheng-yu, LIU Peng-tao. A new ID-based ring signature scheme with constant-size signature [C]//Proc of ICCET. [S. l.]: IEEE Press,2010:579-581.

[9] CAMENISCH J,STADLER M. Efficient group signature schemes for large groups (extended abstract) [C]//Advances in CRYPTO'97. Berlin:Springer-Verlag,1997:410-424.

[10] BELLARE M,MICCIANCIO D,WARINSCHI B. Foundations of group signatures:formal definitions,simplified requirements and a construction based on general assumptions[C]//Proc of EUROCRYPT'03. Berlin:Springer-Verlag,2003:614-629.

[11] BRESSON E,STERN J,SZYDLO M. Threshold ring signatures and applications to Ad hoc groups [C]//Proc of CRYPTO'02. Berlin: Springer-Verlag,2002:465-480.

[12] XIONG Hu,QIN Zhi-guang,LI Fa-gen,*et al*. Identity-based threshold ring signature without pairings[C]//Proc of ICCCAS. [S. l.]:IEEE Press,2008:478-482.

[13] WANG Hu-qun,HAN Sheng-ju. A provably secure threshold ring signature scheme in certificateless cryptography[C]//Proc of ISME. [S. l.]: IEEE Press,2010:105-108.

[14] AGUILAR M C,CAYREL P L,GABORIT P. A new efficient threshold ring signature scheme based on coding theory[J]. IEEE Trans on Information Theory,2011,57(7):4833-4842.

[15] CHOW S S M,HUI L C K,YIU S M. Identity based threshold ringsignature[C]//Lecture Notes in Computer Science, vol 3506. Berlin: Springer-Verlag,2005:697-699.