一种有效基于身份的门限环签密方案*

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：为了设计基于身份的门限环签密方案，利用秘密共享和双线性对技术，提出了一种在标准模型下基于身份的门限环签密方案，并对方案的安全性进行了分析。最后，利用 CDH 问题和 DBDH 问题的困难性，证明了方案在适应性选择消息和身份攻击下的不可伪造性以及在适应性选择密文攻击下的不可区分性。

关键词：门限环签密；双线性对；CDH 问题；DBDH 问题；基于身份的密码学

中图分类号：TP309　　**文献标志码**：A　　**文章编号**：1001-3695(2012)07-2660-05

doi:10.3969/j.issn.1001-3695.2012.07.071

Efficient identity-based threshold ring signcryption scheme

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: In order to design an identity-based threshold ring signcryption, this paper presented an efficient identity-based threshold ring signcryption scheme without random oracles by means of secret sharing and bilinear pairing technique, and analyzed the security of the scheme. Finally, It proved this scheme satisfied indistinguishability against adaptive chosen ciphertext attacks and existential unforgeability against adaptive chosen message and identity attacks in terms of the hardness of DBDH problem and CDH problem.

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

0 引言

1984 年，Shamir[1] 提出了基于身份的公钥密码体制，用以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方案[3,4]。

消息的保密和认证是密码学中最重要的两个研究内容，如何在消息通信过程中同时实现保密和认证是信息安全研究的主要目标之一。1997 年，Zheng[5] 提出了签密的概念，即能够在一个合理的步骤内同时实现加密和签名两项功能，而其通信成本和计算量都低于传统的先签名后加密方法。An 等人[6] 对签密方案的机密性和不可伪造性进行了形式化的描述；Selvi 等人[7] 对 Barbosa 等人[8]、Aranha 等人[9] 以及 Wu 等人[10] 提出的无证书签密方案进行了分析，指出这些方案不满足密文的不可伪造性或机密性；Pandey 等人[11] 利用一般性的基于身份加密和签名方案，构造了一个高效的基于身份签密方案。

匿名性是密码学应用中的另一个重要属性，在实际生活中有着广泛的应用，如在 Ad hoc 网络中需要确保接入用户的信息不被泄露。环签密不仅能够实现消息的不可伪造性和机密性，同时还可以实现签密者的匿名性。Huang 等人[12] 提出了环签密的方案，然而该方案计算效率低；Yu 等人[13] 改进了 Huang 的方案，可是其被证明不是适应性选择密文安全的，甚至不是选择明文安全的；Li 等人[14] 提出了另外一个环签密方案，而该方案依然不是适应性选择密文安全的；Wang 等人[15] 对 Wang 等人[16]、Zhu 等人[17] 提出的环签密方案进行了分析，指出他们的方案是不安全的；Selvi 等人[18] 指出已有的几个基于身份的环签密方案大多是不安全的，并在随机预言模型下提出了一种基于身份的环签密方案。

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，已有的环签密方案大多是在随机预言模型下被证明是安全的，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高的要求，在具体应用中有时无法构造相应的实例。

本文利用秘密共享技术，在标准模型下提出了一种基于身份的门限环签密方案并给出了相应的安全模型，同时利用 CDH 问题和 DBDH 问题的困难性证明了方案的安全性。

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，

收稿日期：2011-12-20；**修回日期**：2012-01-16　　**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资助项目(112102210370)；河南省教育厅科学技术研究重点资助项目(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与信息安全(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.

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

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 $g,g^a,g^b\in G$ 和 $a,b\in_R Z_p^*$,计算 g^{ab}。

DBDH 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 $g^a,g^b,g^c,h\in G$ 和 $a,b,c\in_R Z_p^*$,判定 $h=e(P,P)^{abc}$ 是否成立。

2　基于身份的门限环签密

2.1　形式化定义

基于身份的 (t,n) 门限环签密方案可由以下四个算法组成:

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)签密。(a)各签密者 $ID_i(i=1,\cdots,t)$ 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,然后计算其他各签密者 $ID_j(j\neq i)$ 的秘密分享,并将它们发送给其他签密者,签密者 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;(b)输入环成员身份列表 $L=\{ID_1,\cdots,ID_n\}$、门限值 t、消息 m 以及 t 个签密者的私钥 $\{s_{ID_i}\}(i=1,\cdots,t)$,环签密接收者身份 ID_R,该算法输出在消息 m 下的 (t,n) 门限环签密 C。

d)解签密。输入密文 C、门限值 t、环成员身份列表 L、环签密接收者的私钥 s_{ID_R},如果 C 是一个有效的门限环签密,则输出 true;否则,输出 false。

2.2　基于身份门限环签密(IBTRSC)的安全模型

下面介绍基于身份门限环签密的安全模型,包括不可区分性和不可伪造性。

定义 1　一个基于身份的门限环签密方案在适应性选择密文攻击下是不可区分的(IND-IDTRSC-CCA2),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:

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

b)First phase。敌手 A 可以适应性地向挑战者 C 发出如下一定数量的询问:

(a)Extraction query。敌手 A 选择身份 ID,C 计算其私钥 s_{ID} 并发送给 A。

(b)Signcryption query。敌手 A 选择环成员列表 L、门限值 t、消息 m 以及环签密接收者身份 ID_R 发送给 C,同时 A 也需要指定实际签密者的身份 $ID_i(i=1,\cdots,t;ID_i\in L)$。C 首先运行私钥提取算法生成实际签密者的私钥 s_{ID_i},然后运行签密算法生成 (t,n) 门限环签密并将其发送给 A。

(c)Unsigncryption query。敌手 A 选择环成员列表 L、签密接收者身份 ID_R 和密文 C。C 首先运行 Extract 算法得到 ID_R 的私钥 s_{ID_R},然后运行解签密算法,如果 C 是一个有效的密文,则输出 m;否则,输出 false。

c)Challenge。敌手 A 任选两个相同长度的消息 m_0,m_1,环成员列表 L^* 以及环签密接收者的身份 ID_R^* 发送给 C。这里 A 必须在第一阶段中没有询问 ID_R^* 的私钥。C 任选一位 $b\in\{0,1\}$,计算 m_b 的环签密 C^*,并发送给 A。

d)Second phase。敌手 A 可以像步骤 b)那样发起一定数量的任意询问,但不能对 ID_R^* 的私钥发起询问,同时不能对 C^* 发起 unsigncryption query。

e)Guess。敌手 A 输出一位 b'。如果 $b=b'$,那么 A 赢得游戏。定义敌手 A 获得成功的优势为

$$Adv_A^{IND\text{-}IDTRSC\text{-}CCA2}=2P[b=b']-1$$

定义 2　一个基于身份的门限环签密方案在适应性选择消息和身份攻击下是存在性不可伪造的(EUF-IDTRSC-CMIA),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:

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

b)Query。A 可以像定义 1 中的步骤 b)那样,发起一定数量的任意询问。

c)Forgery。A 输出新元组 (L^*,ID_R^*,C^*),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^*,ID_R^*,C^*) 没有出现在前面的签密询问中。如果 C^* 是一个有效的门限环签密,那么 A 赢得游戏。定义敌手 A 获得成功的优势为

$$Adv_A^{EUF\text{-}IDTRSC\text{-}CMIA}=P[\text{A succeed}]$$

3　标准模型下基于身份的门限环签密方案

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:

a)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 $param=(G,G_T,e,g,g_1,g_2,u',\hat{U},m',\hat{M},H_u,H_m)$,主密钥为 $msk=g_2^\alpha$。

b)私钥提取。给定用户身份 ID,令 $u=H_u(ID)$ 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,$\Phi_{ID}\subseteq\{1,2,\cdots,n_u\}$ 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

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

c)签密。设 $L=\{ID_1,\cdots,ID_n\}$ 为门限环签密中 n 个成员的集合,不妨设实际进行签密的 t 个签密者的身份下标为 $\{1,2,\cdots,t\}$,待签密消息为 m,签密接收者的身份为 ID_R,可以通过执行下面的步骤来生成基于身份的门限环签密:

(a)每个签密者 ID_i 随机选取 $s_i\in Z_p$ 为其子秘密,构造系数为 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 $C_{i,d} = g^{a_{i,d}}(d = 0,1,\cdots,t-1)$并向其他签密者广播，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)签密者 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)每个签密者 ID_i 计算其私有秘密为 $x_i = \sum_{j=1}^{t} s_{j,i}$。

(d)对于 $i \in \{1,2,\cdots,t\}$，设每个签密者 ID_i 的私钥为(d_{i1}, d_{i2})。它计算 $M = H_m(L,m)$，令 $\mathcal{M} \subseteq \{1,2,\cdots,n_m\}$ 为消息 m 的位串中 $M[k] = 1$ 的序号 k 的集合，随机选取 $r_i \in Z_p$，计算 $\sigma_{i1} = e(g_1,g_2)^{r_i}$，$\sigma_{i2} = g^{r_i}$，$\sigma_{i3} = (u' \prod_{j \in \Phi_{\mathrm{ID}_R}} \hat{u}_j)^{r_i}$，$\sigma_{i4} = d_{i1}(m' \prod_{i \in \mathcal{M}} \hat{m}_i)^{x_i\eta_i}$，$\sigma_{i5} = g^{x_i\eta_i}$，$\sigma_{i6} = d_{i2}$，并把$(\sigma_{i1},\sigma_{i2},\sigma_{i3},\sigma_{i4},\sigma_{i5},\sigma_{i6})$发送给 t 个签密者中任一用以产生门限环签密的签密者，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)令 $m \in G_{\mathrm{T}}$ 为待签密消息，该门限环签密者随机选取 $l_1,\cdots,l_n \in Z_p$，计算 $U_i = u' \prod_{j \in \Phi_{\mathrm{ID}_i}} \hat{u}_j (i = 1,\cdots,n)$，$R_1 = \sigma_{16} g^{l_1}$，$\cdots$，$R_t = \sigma_{t6} g^{l_t}$，$R_{t+1} = g^{l_{t+1}}$，$\cdots$，$R_n = g^{l_n}$。令 $\sigma_1 = \prod_{i=1}^{t}\sigma_{i1}\, m$，$\sigma_2 = \prod_{i=1}^{t}\sigma_{i2}$，$\sigma_3 = \prod_{i=1}^{t}\sigma_{i3}$，$\sigma_4 = \prod_{i=1}^{t}\sigma_{i4} \times \prod_{i=1}^{n}(U_i)^{l_i}$，$\sigma_5 = \prod_{i=1}^{t}\sigma_{i5}$，则生成的门限环签密为 $C = (\sigma_1,\cdots,\sigma_5,R_1,\cdots,R_n)$。

d)解签密。设签密接收者 ID_R 的私钥为(d_{R1}, d_{R2})，当收到门限环签密 C 后，进行如下计算：

(a)计算 $m = \sigma_1 \times e(d_{R2},\sigma_3) \times e(d_{R1},\sigma_2)^{-1}$。

(b)计算 $M = H_m(L,m)$，得到消息 m 位串中 $M[k] = 1$ 的序号 k 的集合 $\mathcal{M}$。

(c)当且仅当等式 $e(\sigma_4,g) = e(g_1,g_2)^t e(U_1,R_1)\cdots e(U_n, R_n)e(m' \prod_{i \in \mathcal{M}} m_i, \sigma_5)$ 成立时，C 是一个有效的门限环签密。

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：

$$\sum_{i=1}^{t} x_i\eta_i = \sum_{i=1}^{t} f_i(0) = \sum_{i=1}^{t} s_i$$

b)当签密接收者收到门限环签密 C 后，可进行验证：

$$\sigma_1 = \prod_{i=1}^{t}\sigma_{i1} \times m = e(g_1,g_2)^{\sum_{i=1}^{t} r_i} \times m$$

$$\sigma_2 = \prod_{i=1}^{t}\sigma_{i2} = g^{\sum_{i=1}^{t} r_i}$$

$$\sigma_3 = \prod_{i=1}^{t}\sigma_{i3} = (u' \prod_{j \in \Phi_{\mathrm{ID}_R}} \hat{u}_j)^{\sum_{i=1}^{t} r_i}$$

$$\sigma_4 = \prod_{i=1}^{t}\sigma_{i4} \times \prod_{i=1}^{n}(U_i)^{l_i} = g_2^{ta}(U_1)^{r_{\mathrm{ID}_1}+l_1}\cdots$$

$$(U_t)^{r_{\mathrm{ID}_t}+l_t}(U_{t+1})^{l_{t+1}}\cdots(U_n)^{l_n}(m' \prod_{i \in \mathcal{M}} \hat{m}_i)^{\sum_{i=1}^{t} x_i\eta_i}$$

$$\sigma_5 = \prod_{i=1}^{t}\sigma_{i5} = g^{\sum_{i=1}^{t} x_i\eta_i}$$

因此，可得

$$\sigma_1 \times e(d_{R2},\sigma_3) \times e(d_{R1},\sigma_2)^{-1} = e(g_1,g_2)^{\sum_{i=1}^{t} r_i} \times m \times$$

$$e(g^{r_{\mathrm{ID}_R}}, (u' \prod_{j \in \Phi_{\mathrm{ID}_R}} \hat{u}_j)^{\sum_{i=1}^{t} r_i}) \times e(g_2^a (u' \prod_{j \in \Phi_{\mathrm{ID}_R}} \hat{u}_j)^{r_{\mathrm{ID}_R}}, g^{\sum_{i=1}^{t} r_i})^{-1} = m$$

$$e(\sigma_4,g) = e(\prod_{i=1}^{t}\sigma_{i4} \times \prod_{i=1}^{n}(U_i)^{l_i}, g) = e(g, g_2^{ta}) \times$$

$$e((u_1)^{r_{\mathrm{ID}_1}+l_1}\cdots(U_t)^{r_{\mathrm{ID}_t}+l_t}(U_{t+1})^{l_{t+1}}\cdots(U_n)^{l_n}(m' \prod_{i \in \mathcal{M}} m_i)^{\sum_{i=1}^{t} x_i\eta_i}, g) =$$

$$e(g_1,g_2)^t e(U_1,R_1)\cdots e(U_n,R_n)e(m' \prod_{i \in \mathcal{M}} m_i, g^{\sum_{i=1}^{t} x_i\eta_i}) =$$

$$e(g_1,g_2)^t e(U_1,R_1)\cdots e(U_n,R_n)e(m' \prod_{i \in \mathcal{M}} m_i, \sigma_5)$$

故方案是正确的。

3.3 方案安全性

下面证明方案满足适应性选择密文攻击下的不可区分性以及适应性选择消息和身份攻击下的存在不可伪造性。

定理 1 在 DBDH 困难问题的假设下，方案是 IND-IDTR-SC-CCA2 安全的。

证明 假设敌手 A 能以不可忽略的优势攻击本方案，则能够构造算法 B，B 可以利用 A 解决 DBDH 问题。

给定 B 一个 DBDH 问题的实例(g, g^a, g^b, g^c, h)，它的目标是判断 $h = e(g,g)^{abc}$ 是否成立。B 模仿 A 的挑战者，其过程如下：

a)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 $x' \in_R Z_{l_u}$及长度为 n_u 的向量 $\boldsymbol{X} = (x_i)$，其中 $x_i \in_R Z_{l_u}$；选择及长度为 n_m 的向量 $\boldsymbol{Z} = (z_k)$，其中 $z_k \in_R Z_{l_m}$；最后 B 选择 $y', w' \in_R Z_p$，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 $y_i, w_i \in_R Z_p$。

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

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

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

算法 B 构造上面方案中的公开参数如下：

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

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

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

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

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

然后算法 B 将公开参数发送给敌手 A。

b)阶段 1。当敌手 A 发起一定数量的询问时，算法 B 进行如下响应：

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

$$d_{\mathrm{ID}} = (d_1,d_2) = (g_1^{-J(\mathrm{ID})/F(\mathrm{ID})}(u' \prod_{i \in \Phi_{\mathrm{ID}}} u_i)^{r_u}, g_1^{-1/F(\mathrm{ID})} g^{r_u})$$

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

$$d_1 = g_1^{-J(\mathrm{ID})/F(\mathrm{ID})}(u' \prod_{i \in \Phi_{\mathrm{ID}}} u_i)^{r_u} =$$

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

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

$$d_2 = g_1^{-1/F(\mathrm{ID})} g^{r_u} = g^{r_u - a/F(\mathrm{ID})} = g^{\tilde{r}_u}$$

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 $F(\mathrm{ID}) = 0 \bmod p$，上面的计算将无法进行，B 将失败退出。

(b)签密询问。当敌手 A 询问环成员身份为 $L=\{\mathrm{ID}_1,\cdots,\mathrm{ID}_n\}$、门限值为 $t(t<n)$、消息为 m、实际签密者为 $\mathrm{ID}_i(i=1,\cdots,t)$以及环签密接收者为 ID_R 的门限环签密时,算法 B 首先计算 $M=H_m(L,m)$,然后按照如下步骤输出门限环签密:

①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 $f(x)=a_0+a_1x+\cdots+a_{t-1}x^{t-1}$,其中 $s=a_0$。

②假定对于实际签密者 $\mathrm{ID}_i(i=1,\cdots,t)$,满足 $F(\mathrm{ID}_i)\neq 0 \bmod p$,则算法 B 按照私钥询问中的方法构造它们的私钥,计算各签密者 $\mathrm{ID}_i(i=1,\cdots,t)$的私有秘密 $x_i=f(i)$,然后利用签密算法生成相应的门限环签密 C。

③如果条件 $F(\mathrm{ID}_i)\neq 0 \bmod p(i=1,\cdots,t)$不成立,那么算法 B 也可以像在私钥询问中构造私钥的方法那样构造该门限环签密。假定 $K(M)\neq 0 \bmod p$,算法 B 随机选择 $r,r_1,\cdots,r_n,r_m\in Z_p$,计算:

$$\sigma_1=e(g_1,g_2)^r\times m,\sigma_2=g^r,\sigma_3=(u'\prod_{j\in\Phi_{\mathrm{ID}_R}}\hat{u}_j)^r$$

$$\sigma_4=(\prod_{i=1}^{n}(U_i)^{r_i})g_1^{-tL(M)/K(M)}(m'\prod_{i\in\mathcal{M}}m_i)^{r_m}=$$

$$g_2^{ta}(\prod_{i=1}^{n}(U_i)^{r_i})(m'\prod_{i\in\mathcal{M}}m_i)^{\tilde{r}_m}$$

$$\sigma_5=g^{r_m}$$

$$R_1=g^{r_1},\cdots,R_n=g^{r_n}$$

其中,$\tilde{r}_m=r_m-a/K(M)$,可见 $C=(\sigma_1,\cdots,\sigma_5,R_1,\cdots,R_n)$是一个有效的门限环签密。如果 $K(M)=0 \bmod p$,上面的计算将无法进行,B 将失败退出。

(c)解签密询问。当敌手 A 发起在环成员列表 L、环签密接收者身份为 ID_R 以及密文 C 下的解签密询问时,算法 B 首先运行私钥提取算法得到 ID_R 的私钥 d_{ID_R},然后运行解签密算法,如果 C 是一个有效的密文,则输出 m;否则,输出 false。

c)挑战。在第一阶段后,敌手 A 任取两个相同长度的消息 m_0、m_1,并将环成员列表 $L^*=\{\mathrm{ID}_1^*,\cdots,\mathrm{ID}_n^*\}$以及环签密接收者的身份 ID_R^* 发送给算法 B。如果 A 在第一阶段询问了 ID_R^* 的私钥,则 B 将失败退出。B 任选一位 $b\in\{0,1\}$,如果 $K(M_b)\neq 0 \bmod p$,$F(\mathrm{ID}_R^*)\neq 0 \bmod p$,那么 B 将失败退出。如果 L^* 中不存在 t 个身份 ID^*,满足 $F(\mathrm{ID}^*)\neq 0 \bmod p$,那么 B 将失败退出;否则,为描述方便起见,不妨设这 t 个身份为 $\mathrm{ID}_1^*,\cdots,\mathrm{ID}_t^*$。B 随机选取 $r,r_1,\cdots,r_n,r_m\in Z_p$,构造如下:

$$\sigma_1^*=h\times m_b,\sigma_2^*=g^c$$

$$\sigma_3^*=g^{cJ(\mathrm{ID}_R^*)}=(u'\prod_{j\in\Phi_{\mathrm{ID}_R^*}}\hat{u}_j)^c$$

$$\sigma_4^*=\prod_{i=1}^{t}g_1^{\frac{-J(\mathrm{ID}_i^*)}{F(\mathrm{ID}_i^*)}}(g_2^{F(\mathrm{ID}_i^*)}g^{J(\mathrm{ID}_i^*)})^{r_i}\times$$

$$\prod_{i=t+1}^{n}(g_2^{F(\mathrm{ID}_i^*)}g^{J(\mathrm{ID}_i^*)})^{r_i}\times g^{r_mL(M_b)}=$$

$$g_2^{ta}\prod_{i=1}^{t}(u'\prod_{j\in\Phi_{\mathrm{ID}_i^*}}\hat{u}_j)^{\tilde{r}_i}\cdot\prod_{i=t+1}^{n}(u'\prod_{j\in\Phi_{\mathrm{ID}_i^*}}\hat{u}_j)^{r_i}(m'\prod_{j\in\mathcal{M}}\hat{m}_j)^{r_m}$$

$$\sigma_5^*=g^{r_m}$$

$$R_1^*=g^{\tilde{r}_1},\cdots,R_t^*=g^{\tilde{r}_t},R_{t+1}^*=g^{r_{t+1}},\cdots,R_n^*=g^{r_n}$$

其中,$\tilde{r}_i=r_i-a/F(\mathrm{ID}_i^*)(i=1,\cdots,t)$,如果 $h=e(g,g)^{abc}$,可知 C^* 是一个有效的门限环签密。

d)阶段 2。敌手 A 可以如同阶段 1 那样,发出一定数量的私钥询问、签密询问以及解密询问,但是 A 不能询问 ID_R^* 的私钥以及对 C^* 进行解签密询问。

e)猜测。最后,敌手 A 输出对 b 的猜测 b'。如果 $b=b'$,则 B 输出 1,将 $h=e(g,g)^{abc}$ 作为 DBDH 问题的解;否则,B 输出 0,终止游戏。因此,如果存在一个敌手能够以不可忽略的概率进行 CCA2 攻击,那么就存在一个有效的算法能够以不可忽略的概率解决 DBDH 问题,而这与 DBDH 是一个困难问题相矛盾,故方案是 IND-IDTRSC-CCA2 安全的。

定理 2　在 CDH 困难问题的假设下,方案是 EUF-IDTRSC-CMIA 安全的。

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,具体过程如下:

a)系统初始化。构造与前面证明中相同的系统公开参数,然后算法 B 将公开参数发送给敌手 A。

b)询问。敌手 A 可如同定理 1 证明中那样,适应性发起一定数量的私钥询问、签密询问以及解签密询问。

c)伪造。敌手 A 输出在环成员列表 $L^*=\{\mathrm{ID}_1^*,\cdots,\mathrm{ID}_n^*\}$、门限值 t、消息 m^* 以及环签密接收者身份为 ID_R^* 下的伪造门限环签密 C^*。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 $M^*=H_m(L,m^*)$。

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

$$\left(\frac{\sigma_4^*}{R_1^{J(\mathrm{ID}_1^*)}\cdots R_n^{J(\mathrm{ID}_n^*)}R_m^{L(M^*)}}\right)^{1/t}=$$

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

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

这就是 CDH 问题的解。

因此,如果存在一个敌手能够以不可忽略的概率伪造一个有效的门限环签密,那么就存在一个算法能够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,故方案是 EUF-IDTRSC-CMIA 安全的。

4　结束语

本文利用秘密共享技术提出了一种门限环签密方案,而现有基于身份环签密方案的安全性大多是在随机模型下证明的,同时对于门限环签密方案的研究也不多。本文在标准模型下设计了一个基于身份的门限环签密方案,通过对方案的安全性进行证明,指出方案在 DBDH 和 CDH 困难问题的假设下满足适应性选择密文攻击下的不可区分性以及适应性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可靠的。

参考文献:

[1] SHAMIR A. Identity-based cryptosystems and signature schemes [C]//Proc of CRYPTO on Advances in cryptology. New York: Springer-Verlag, 1985: 47-53.

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

229.

[3] WATERS B. Efficient identity-based encryption without random oracles[C]//Proc of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques. Berlin: Springer-Verlag, 2005:114-127.

[4] PATERSON K G, SCHULDT J C N. Efficient identity-based signatures secure in the standard model[C]//Proc of the 11th Australasian Conference on Information Security and Privacy. Berlin: Springer-Verlag, 2006:207-222.

[5] ZHENG Yu-liang. Digital signcryption or how to achieve cost(signature & encryption) < < cost(signature) + cost(encryption)[C]// Proc of the 17th Annual International Cryptology Conference on Advances in Cryptology. Berlin: Springer-Verlag, 1997:165-179.

[6] AN J H, DODIS Y, RABIN T. On the security of joint signature and encryption[C]//Proc of International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Crytology. Berlin: Springer-Verlag, 2002:83-107.

[7] SELVI S S D, VIVEK S S, RANGAN C P. Cryptanalysis of certificateless signcryption schemes and an efficient construction without pairing [C]//Proc of the 5th International Conference on Information Security and Cryptology. Berlin: Springer-Verlag, 2010:75-92.

[8] BARBOSA M, FARSHIM P. Certificateless signcryption[C]//Proc of ACM Symposium on Information, Computer and Communications Security. New York: ACM Press, 2008:369-372.

[9] ARANHA D, CASTRO R, LÓPEZ J, *et al*. Efficient certificateless signcryption[C]//Proc of Beazilian Symposium on Information Security and Computer Systems. 2008:257-258.

[10] WU Chen-huang, CHEN Zhi-xiong. A new efficient certificateless signcryption scheme[C]//Proc of International Symposium on Information Science and Engineering. Washington DC: IEEE Computer Society, 2008:661-664.

[11] PANDEY S K, BARUA R. Construction of identity based signcryption schemes[C]//Proc of the 11th International Conference on Information Security Applications. Berlin: Springer-Verlag, 2010:1-14.

[12] HUANG Xin-yi, SUSILO W, MU Yi, *et al*. Identity-based ring signcryption schemes: cryptographic primitives for preserving privacy and authenticity in the ubiquitous world[C]//Proc of the 19th International Conference on Advanced Information Networking and Application. Washington DC: IEEE Computer Society, 2005:649-654.

[13] YU Yong, LI Fa-gen, XU Chun-xiang, *et al*. An efficient identity-based anonymous signcryption scheme[J]. Wuhan University Journal of Natural Sciences, 2008, 13(6):670-674.

[14] LI Fa-gen, SHIRASE M, TAKAGI T. Analysis and improvement of authenticatable ring signcryption scheme[J]. Journal of Shanghai Jiaotong University(Science), 2008, 13(6):679-683.

[15] WANG Hua-quan, YU Hong. Cryptanalysis of two ring signcryption schemes[M]//YUNG Mo-ti, LIU Peng, LIN Dong-dai. Information Security and Cryptology. Berlin: Springer-Verlag, 2009:41-46.

[16] WANG Ling-ling, ZHANG Guo-yin, MA Chun-guang. A secure ring signcryption scheme for private and anonymous communication[C]// Proc of IFIP International Conference on Network and Parallel Computing Workshops. Washington DC: IEEE Computer Society, 2007:107-111.

[17] ZHU Zhen-chao, ZHANG Yu-qing, WANG Feng-jiao. An efficient identity-based ring signcryption scheme[EB/OL]. (2008-06-03). http://eprint.iacr.org/2008/254.pdf.

[18] SELVI S S D, VIVEK S S, RANGAN C P. On the security of identity based ring signcryption schemes[C]//Proc of the 12th International Conference on Information Security. Berlin: Springer-Verlag, 2009: 310-325.