标准模型下可证安全的基于身份的门限环签密方案

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

摘 要 签密是一个能够同时提供认证性和保密性的密码学术语,而它却比分别签名和加密具有更低的计算成本。环签密除具有签密的一般属性外,还具有匿名性。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,通过计算 Diffie-Hellman 问题和判定性 Diffie-Hellman 问题的困难性,证明了该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,计算 Diffie-Hellman 问题,判定性 Diffie-Hellman 问题,基于身份的密码学
中图法分类号 TP309 **文献标识码** A

Provably Secure Identity-based Threshold Ring Signcryption Scheme in Standard Model

SUN Hua[1] WANG Ai-min[1] ZHENG Xue-feng[2]
(School of Computer and Information Engineering, Anyang Normal University, Anyang 455000, China)[1]
(School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China)[2]

Abstract Signcryption is a cryptographic primitive which can provide authentication and confidentiality simultaneously with a computational cost lower than signing and encryption respectively, while the ring signcryption has anonymity in addition to authentication and confidentiality. 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 gave security analysis of the scheme. At last, we proved this scheme satisfies 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.

Keywords Threshold ring signcryption, Bilinear pairing, Computational Diffie-Hellman problem, Decisional bilinear Diffie-Hellman problem, Identity based cryptography

1984年,Shamir[1]创造性地提出了基于身份的公钥密码学,解决了传统公钥密码体制中庞大的公钥证书存储和验证开销问题。在基于身份的密码体制中,用户的公钥为能够标识用户身份的信息,如用户的姓名、身份证号码等,用户的私钥则由可信第三方 PKG(Private Key Generator)生成。2001年,Boneh 和 Franklin[2]基于超奇异椭圆曲线上的双线性对技术提出了第一个高效实用的基于身份的加密方案,他们的工作开创了身份密码学研究的新时代。此后许多利用双线性对技术构造的基于身份密码方案[3,4]被相继提出。

保密和认证是密码学中两个重要的安全目标,在许多密码应用中需要同时取得这两个目标,然而传统的实现方法不仅计算量大,而且效率较低。1997年,Zheng[5]提出了签密这一密码原语,它能够同时取得这两个安全目标,而其计算量和通信成本却低于传统的实现方法。

门限签密方面,2004年,Duan 等人[6]提出了基于身份的门限签密方案,可是该方案采取分享 PKG 主密钥的方法,这样容易使 PKG 成为瓶颈。2005年,Peng 等人[7]提出了另外一个基于身份的门限签密方案,该方案克服了前一方案的弱点,即采取分享一个身份对应的私钥而不是分享 PKG 的主密钥,但他们的方案不能够提供前向安全性。2008年,Li 等人[8]利用双线性对技术提出了第一个可证安全的基于身份的门限签密方案,同时在随机预言模型下可证了方案的语义安全性和不可伪造性。然而,Zhu 等人[9]在其文章中指出 Li 等人的方案并不能抵抗存在性伪造攻击。

匿名性是密码学应用中的另一个重要属性,在现实中有着广泛的应用。环签密不仅能够实现消息的机密性和认证,而且还能够实现签密者的匿名性。Huang 等人[10]首先提出了基于身份的环签密方案,可是该方案不具有身份认证性,并且计算量太大。2008年,Zhang 等人[11]提出了可认证的基于身份的环签密方案,签密发送者可以向接收者证明该签密确

到稿日期:2012-05-21 返修日期:2012-09-22 本文受国家自然科学基金资助项目(61075039,61170244),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)资助。

孙 华(1980—),男,博士,讲师,CCF 会员,主要研究方向为密码学与信息安全;王爱民(1957—),男,博士,教授,主要研究方向为可信计算、数据挖掘;郑雪峰(1951—),男,教授,主要研究方向为网络与信息安全。

实是由他产生的，可是该方案不能抵抗适应性选择密文攻击。同年，Zhun 等人[12]提出了一个基于身份的环签名和环签密方案，但是该方案不能抵抗适应性选择明文攻击。随后，Zhu 等人[13]在随机预言模型下提出了一种基于身份的环签密方案，然而该方案依然不是适应性选择密文攻击下安全的。2009 年，Sharmila 等人[14]指出已有的几个基于身份的环签密方案大都是不安全的，并在随机预言模型下提出了一种基于身份的环签密方案。

2011 年，罗大文等人[15]提出了一种基于身份的门限环签密方案，然而该方案是在随机预言模型下可证安全的。目前，已有的环签密方案普遍是在随机预言模型下可证安全的，由于在随机预言模型中把 Hash 函数看成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，因此在随机预言模型下可证安全的方案在实际环境中不一定是安全的，故在标准模型下构造高效可证安全的门限环签密方案更有实际意义。

本文首先给出基于身份门限环签密的形式化定义和安全模型，然后利用秘密共享技术提出了一个在标准模型下可证安全的基于身份门限环签密方案（IBTRSC，Identity-Based Threshold Ring Signcryption），最后在所定义的安全模型下基于困难问题假设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，双线性对是满足如下性质的映射 $e: G\times G \to G_T$：

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

2. 非退化性：$e(g,g)\neq 1$；

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

双线性映射可以通过有限域上的超奇异椭圆曲线中的 Well 对或 Tate 对推导出来。

1.2 困难问题假设

计算 Diffie-Hellman(CDH)问题：已知 g 是群 G 的生成元，给定 $g,g^a,g^b\in G$，其中 $a,b\in_R Z_p^*$，计算 g^{ab}。

判定性 Diffie-Hellman(DBDH)问题：已知 g 是群 G 的生成元，给定 $g^a,g^b,g^c\in G, h\in G_T$，其中 $a,b,c\in_R Z_p^*$，判定 $h=e(P,P)^{abc}$ 是否成立。

2 IBTRSC 体制定义

2.1 IBTRSC 的形式化定义

定义 1 设 $P=\{P_1,\cdots,P_n\}$ 为环签密中 n 个成员的集合，相应的身份为 $ID_i(i=1,\cdots,n)$，门限值为 t，假设实际进行签密的 t 个签密者的身份为 $ID_i(i=1,\cdots,t)$，待签密消息为 m，环签密接收者的身份为 ID_R，则 (t,n)-IBTRSC 方案由以下算法组成。

1）系统参数产生算法：给定安全参数 k，算法输出系统参数 *params* 以及相应的主密钥 *msk*。其中 *params* 是公开的，而 *msk* 是保密的。

2）私钥产生算法：输入系统参数 *params*、主密钥 *msk* 和用户身份 ID，算法输出身份 ID 的私钥 d_{ID}。

3）门限环签密产生算法：首先，输入门限值 t、环签密成员的规模 n、实际签密者的子秘密 s_i，输出实际签密者的私有秘密 x_i；其次，输入环成员身份列表 $L=\{ID_1,\cdots,ID_n\}$、消息 m、实际签密者的私钥、门限环签密接收者身份 ID_R，输出部分环签密；最后，输入有效的 t 个部分环签密，任一实际签密者通过计算输出在消息 m 下的 (t,n) 门限环签密 C。

4）解签密算法：输入门限环签密 C、环成员身份列表 L、门限环签密接收者的私钥 d_{ID_R}，如果 C 是一个有效的门限环签密，则输出 1；否则输出 0。

2.2 IBTRSC 的安全模型

根据门限环签密方案的安全目标，下面通过挑战者 $\mathscr{C}$ 和敌手 $\mathscr{A}$ 之间的游戏，我们可以定义基于身份门限环签密方案的安全模型。

定义 2 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-IBTRSC-CCA2），如果没有概率多项式时间的敌手 $\mathscr{A}$ 在下面的游戏中获得不可忽略的优势：

准备阶段：挑战者 $\mathscr{C}$ 运行系统参数产生算法得到系统参数 *params* 并发送给敌手 $\mathscr{A}$，保存主密钥 *msk*。

第一阶段　敌手 $\mathscr{A}$ 可以适应性地向挑战者 C 发出一定数量的如下询问：

私钥询问：敌手 $\mathscr{A}$ 可以询问任何身份 ID 的私钥 d_{ID}，$\mathscr{C}$ 运行私钥产生算法得到其私钥并发送给 $\mathscr{A}$。

签密询问：敌手 $\mathscr{A}$ 选择环成员列表 L、门限值 t、消息 m 以及门限环签密接收者身份 ID_R 发送给 $\mathscr{C}$，同时 $\mathscr{A}$ 指定实际签密者的身份 $ID_i(i=1,\cdots,n), ID_i\in L$。$\mathscr{C}$ 首先运行私钥产生算法生成实际签密者的私钥 d_{ID_i}，然后运行门限环签密产生算法得到门限环签密 C 并将其发送给 $\mathscr{A}$。

解签密询问：敌手 $\mathscr{A}$ 选择环成员列表 L、门限环签密接收者身份 ID_R 和门限环签密 C。$\mathscr{C}$ 首先运行私钥产生算法得到 ID_R 的私钥 d_{ID_R}，然后运行解签密算法，如果 C 是一个有效的门限环签密，则输出 m，否则，输出 false。

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

第二阶段　敌手 $\mathscr{A}$ 可以像第一阶段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^* 发起解签密询问。

猜测阶段：敌手 $\mathscr{A}$ 输出一位 b'。如果 $b=b'$，那么 $\mathscr{A}$ 赢得游戏。我们定义敌手 $\mathscr{A}$ 获得成功的优势为：

$$Adv_{\mathscr{A}}^{IND\text{-}IBTRSC\text{-}CCA2}=2P[b=b']-1$$

定义 3 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-IBTRSC-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：

准备阶段：挑战者 $\mathscr{C}$ 运行系统参数产生算法得到系统参数 *params* 并发送给敌手 $\mathscr{A}$，保存主密钥 *msk*。

询问阶段：$\mathscr{A}$ 可以像定义 2 中的第一阶段那样，发起一定数量的任意询问。

伪造阶段：$\mathscr{A}$ 输出新元组 (L^*,ID_R^*,C^*)，这里的限制条件是至多询问了 L^* 中 $t-1$ 个身份的私钥且 (L^*,ID_R^*) 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 $\mathcal{A}$ 赢得游戏。我们定义敌手 $\mathcal{A}$ 获得成功的优势为：

$Adv_{\mathcal{A}}^{EUF\text{-}IBTRSC\text{-}CMIA}=P[\mathcal{A}\text{succeeds}]$

3 本文的 IBTRSC 方案

3.1 方案描述

令 G、G_T 是阶为素数 p 的循环群，g 是群 G 的生成元，$e:G\times G\to G_T$ 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。

1)系统参数产生算法

PKG 选取 $\alpha\in_R Z_p$，计算 $g_1=g^\alpha$。选取 $u'\in_R Z_p$，g_2，$m'\in_R G$，n_u 维向量 $\hat{U}=(u_i)$，n_m 维向量 $\hat{M}=(m_i)$，其中 $u_i\in_R Z_p$，$m_i\in_R G$。令 $z_1=e(g_1,g_2)$，$z_2=e(g,g_2)$，则系统公开参数为 $params=(G,G_T,e,g,g_1,g_2,u',\hat{U},m',\hat{M},H_u,H_m,z_1,z_2)$，主密钥为 $msk=a$。

2)私钥产生算法

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 选取 $r\in_R Z_p$，计算身份 ID 的私钥为：

$$d_{ID}=(d_1,d_2)=(g_2^{\alpha+r(u'+\sum_{i\in\Phi_{ID}}u_i)},z_2^r)$$

然后通过安全通道将其发送给用户。收到私钥 d_{ID} 后，用户首先对其进行验证，若等式 $e(g,d_1)=z_1 d_2^{(u'+\sum_{i\in\Phi_{ID}}u_i)}$ 成立，则可确定私钥是 PKG 产生的；否则，用户将重新向 PKG 询问其私钥。

3)门限环签密产生算法

设 $L=\{ID_1,\cdots,ID_n\}$ 为门限环签密中 n 个成员身份的集合，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：

①每个签密者 ID_i 选取 $s_i\in_R Z_p$ 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 $C_{i,d}=g^{a_{i,d}}$ $(d=0,1,\cdots,t-1)$ 并向其它签密者广播，计算分享 $s_{i,j}=f_i(j)$，然后把它们发送给其它成员 ID_j $(j=1,2,\cdots,t;j\neq i)$，而自己保留 $s_{i,i}=f_i(i)$。

②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。

③每个签密者 ID_i 计算其私有秘密为 $x_i=\sum_{j=1}^{t}s_{j,i}$。

④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，选取 $r_i\in_R Z_p$，计算 $\sigma_{i1}=e(g_1,g_2)^{r_i}=z_1^{r_i}$，$\sigma_{i2}=g^{r_i}$，$\sigma_{i3}=r_i(u'+\sum_{j\in\Phi_{ID_R}}u_j)$，$\sigma_{i4}=d_{i1}(m'\prod_{i\in\mathcal{M}}m_i)^{x_i\eta_i}$，$\sigma_{i5}=g^{x_i\eta_i}$，$\sigma_{i6}=d_{i2}$，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。

⑤令 $m\in G_T$ 为待签密消息，该门限环签密者选取 $l_1,\cdots,l_n\in_R Z_p$，计算 $U_i=(u'+\sum_{j\in\Phi_{ID_i}}u_j)$，$i=1,\cdots,n$，$R_1=\sigma_{16}z_2^{l_1},\cdots,R_t=\sigma_{t6}z_2^{l_t}$，$R_{t+1}=z_2^{l_{t+1}},\cdots,R_n=z_2^{l_n}$。令 $\sigma_1=\prod_{i=1}^{t}\sigma_{i1}\cdot m$，$\sigma_2=\prod_{i=1}^{t}\sigma_{i2}$，$\sigma_3=\sum_{i=1}^{t}\sigma_{i3}$，$\sigma_4=\prod_{i=1}^{t}\sigma_{i4}\cdot g_2^{\sum_{i=1}^{n}l_i(U_i)}$，$\sigma_5=\prod_{i=1}^{t}\sigma_{i5}$，则生成的门限环签密为 $C=(\sigma_1,\cdots,\sigma_5,R_1,\cdots,R_n)$。

4)解签密算法

设门限环签密接收者 ID_R 的私钥为 (d_{R_1},d_{R_2})，当收到门限环签密 C 后，其进行如下计算：

①计算 $m=\sigma_1\cdot(d_{R_2})^{\sigma_3}\cdot e(d_{R_1},\sigma_2)^{-1}$。

②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 $\mathcal{M}$。

③当且仅当等式 $e(\sigma_4,g)=e(g_1,g_2)^t\cdot e(m'\prod_{i\in\mathcal{M}}m_i,\sigma_5)\cdot\prod_{i=1}^{n}(R_i)^{U_i}$ 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。

①根据秘密共享技术，有：

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

②当签密接收者收到门限环签密 C 后，可进行验证：

$$\sigma_1=\prod_{i=1}^{t}\sigma_{i1}\cdot m=z_1^{\sum_{i=1}^{t}r_i}\cdot m$$

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

$$\sigma_3=\sum_{i=1}^{t}\sigma_{i3}=\sum_{i=1}^{t}r_i\cdot(u'+\sum_{j\in\Phi_{ID_R}}u_j)$$

$$\sigma_4=\prod_{i=1}^{t}\sigma_{i4}\cdot g_2^{\sum_{i=1}^{n}l_i(U_i)}$$

$$=g_2^{\alpha r+\sum_{i=1}^{t}(r_{ID_i}+l_i)\cdot(U_i)+\sum_{i=t+1}^{n}l_i(U_i)}\cdot(m'\prod_{i\in\mathcal{M}}m_i)^{\sum_{i=1}^{t}x_i\eta_i}$$

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

因此，可得：

$$\sigma_1\cdot(d_{R_2})^{\sigma_3}\cdot e(d_{R_1},\sigma_2)^{-1}=e(g_1,g_2)^{\sum_{i=1}^{t}r_i}\cdot m\cdot(e(g,g_2)^{r_{ID_R}})^{\sum_{i=1}^{t}r_i\cdot(U_{ID_R})}\cdot e(g_2^{\alpha r_{ID_R}(U_{ID_R})},g^{\sum_{i=1}^{t}r_i})^{-1}=m$$

$$e(\sigma_4,g)=e(g_2^{\alpha r+\sum_{i=1}^{t}(r_{ID_i}+l_i)\cdot(U_i)+\sum_{i=t+1}^{n}l_i(U_i)}(m'\prod_{i\in\mathcal{M}}m_i)^{\sum_{i=1}^{t}x_i\eta_i},g)$$

$$=e(g,g_2^{\alpha r})\cdot e((m'\prod_{i\in\mathcal{M}}m_i)^{\sum_{i=1}^{t}x_i\eta_i},g)\cdot\prod_{i=1}^{n}(R_i)^{U_i}$$

$$=e(g_1,g_2)^t\cdot e(m'\prod_{i\in\mathcal{M}}m_i,\sigma_5)\cdot\prod_{i=1}^{n}(R_i)^{U_i}$$

故方案是正确的。

3.3 方案安全性

下面证明本文方案满足不可区分性和不可伪造性。

定理 1 在 DBDH 困难问题假设下，本文的方案是 IND-IDTRSC-CCA2 安全的。

证明：假设敌手 $\mathcal{A}$ 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 $\mathcal{A}$ 解决 DBDH 问题，从而导致矛盾。

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

系统初始化：B 设定 $l_u=2(q_e+q_s)$、$l_m=2q_s$，其中 q_e 是 $\mathcal{A}$ 私钥询问的次数，q_s 是 $\mathcal{A}$ 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 $x'\in_R Z_{l_u}$ 和长度为 n_u 的向量 $X=(x_i)$，其中 $x_i\in_R Z_{l_u}$；选择 $z'\in_R Z_{l_m}$ 和长度为 n_m 的向量 $Z=(z_k)$，其中 $z_k\in_R Z_{l_m}$。最后B选择 $w'\in_R Z_p$ 和长度为 n_m 的向量 $W=(w_i)$，其中 $w_i\in_R Z_p$。

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

$$F(ID)=x'+\sum_{i\in\Phi}x_i-l_uk_u$$

$$K(M)=z'+\sum_{i\in\mathcal{M}}z_i-l_mk_m$$

$$L(M)=w'+\sum_{i\in\mathcal{M}}w_i$$

算法B按照如下方式构造上面方案中的公开参数：

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

$$u'=x'-l_uk_u,u_i=x_i,1\leqslant i\leqslant n_u$$

$$m'=g_2^{-l_mk_m+z'}g^{w'}$$

$$m_i=g_2^{z_i}g^{w_i},1\leqslant i\leqslant n_m$$

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，同时有下面的等式：

$$g_2^a=g^{ab},F(ID)=u'+\sum_{i\in\Phi}u_i,m'\prod_{i\in\mathcal{M}}m_k=g_2^{K(M)}g^{L(M)}$$

然后算法B将公开参数发送给敌手 $\mathcal{A}$。

第一阶段　当敌手 $\mathcal{A}$ 发起一定数量的询问时，算法B进行如下响应：

①私钥询问：当敌手 $\mathcal{A}$ 对身份为 ID 的私钥进行询问时，虽然算法B不知道主密钥，但是在假定 $F(ID)\neq 0 \bmod p$ 的情况下，B也能够构造其私钥 d_{ID}。B选取 $r\in_R Z_p$，并计算：

$$d_{ID}=(d_1,d_2)$$

$$=(g_1^{-1}(gg_2)^{r(u'+\sum_{i\in\Phi_{ID}}u_i)},e(gg_2,g^rg_1^{-1/(u'+\sum_{i\in\Phi_{ID}}u_i)}))$$

算法B将 d_{ID} 发送给 $\mathcal{A}$，$\mathcal{A}$ 对其进行验证。

$$e(g,d_1)=e(g,g_1^{-1}(gg_2)^{r(u'+\sum_{i\in\Phi_{ID}}u_i)})$$

$$=e(g_1,g_2)e(gg_2,g^rg_1^{-1/F(ID)})^{F(ID)}$$

$$=z_1d_2^{F(ID)}=z_1d_2^{(u'+\sum_{i\in\Phi_{ID}}u_i)}$$

对于敌手 $\mathcal{A}$ 而言，算法B所产生的私钥与真实挑战者所产生的私钥是不可区分的。如果 $F(ID)=0 \bmod p$，上面的计算将无法进行，B将失败退出。

②签密询问：当敌手 $\mathcal{A}$ 询问环成员身份为 $L=\{ID_1,\cdots,ID_n\}$、门限值为 $t(t<n)$、消息为 m、实际签密者为 $ID_i(i=1,\cdots,t)$ 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：

i)算法B选择 $s,a_0,a_1,\cdots,a_{t-1}\in_R Z_p$，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 $s=a_0$。

ii)假定实际签密者 $ID_i(i=1,\cdots,t)$ 满足 $F(ID_i)\neq 0 \bmod p$，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 $ID_i(i=1,\cdots,t)$ 的私有秘密 $x_i=f(i)$，然后利用门限环签密产生算法生成相应的门限环签密 C。

iii)如果条件 $F(ID_i)\neq 0 \bmod p,i=1,\cdots,t$ 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选择 $r,r_1,\cdots,r_n,r_m\in_R Z_p$，计算：

$$\sigma_1=e(g_1,g_2)^r\cdot m$$

$$\sigma_2=g^r$$

$$\sigma_3=r(u'+\sum_{j\in\Phi_{ID_R}}u_j)$$

$$\sigma_4=g_2^{\sum_{i=1}^{n}r_i(U_i)}g_1^{-tL(M)/K(M)}(m'\prod_{i\in\mathcal{M}}m_i)^{r_m}$$

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

$$\sigma_5=g_1^{-t/K(M)}g^{r_m}=g^{\tilde{r}_m}$$

$$R_1=z_2^{r_1},\cdots,R_n=z_2^{r_n}$$

其中 $\tilde{r}_m=r_m-ta/K(M)$，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 $K(M)=0 \bmod p$，则上面的计算将无法进行，B将失败退出。

③解签密询问：当敌手 $\mathcal{A}$ 发起在环成员列表 L、门限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。

挑战阶段：在第一阶段后，敌手 $\mathcal{A}$ 任取两个相同长度的消息 m_0、m_1，并将环成员列表 $L^*=\{ID_1^*,\cdots,ID_n^*\}$ 以及门限环签密接收者的身份 ID_R^* 发送给算法B。如果 $\mathcal{A}$ 在第一阶段询问了 ID_R^* 的私钥，那么B将失败退出；B任选一位 $b\in\{0,1\}$，如果 $K(M_b)=0 \bmod p$，那么B将失败退出；如果 $F(ID_R^*)\neq 0 \bmod p$，那么B将失败退出。否则，B选取 $r_1,\cdots,r_n,r_m\in_R Z_P$，构造如下：

$$\sigma_1^*=h\cdot m_b$$

$$\sigma_2^*=g^c$$

$$\sigma_3^*=c(u'+\sum_{j\in\Phi_{ID_R^*}}u_j)=cF(ID_R^*)=0$$

$$\sigma_4^*=g_2^{\sum_{i=1}^{n}r_i(U_i)}g_1^{-tL(M_b)/K(M_b)}(m'\prod_{i\in\mathcal{M}}m_i)^{r_m}$$

$$=g_2^{ta+\sum_{i=1}^{t}r_i(U_i)}(m'\prod_{i\in\mathcal{M}}m_i)^{\tilde{r}_m}$$

$$\sigma_5^*=g_1^{-t/K(M_b)}g^{r_m}=g^{\tilde{r}_m}$$

$$R_1^*=z_2^{r_1},\cdots,R_2^*=z_2^{r_n}$$

其中 $\tilde{r}_m=r_m-ta/K(M_b)$，如果 $h=e(g,g)^{abc}$，则可知 $C^*=(\sigma_1^*,\cdots,\sigma_5^*,R_1^*,\cdots,R_2^*)$ 是一个有效的门限环签密。

第二阶段　敌手 $\mathcal{A}$ 可以同阶段1那样发出一定数量的私钥询问、签密询问以及解签密询问，但是 $\mathcal{A}$ 不能询问 ID_R^* 的私钥以及对 C^* 进行解签密询问。

猜测阶段：最后，敌手 $\mathcal{A}$ 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，如果存在一个能够以不可忽略的概率进行CCA2攻击的敌手，那么就存在一个能够以不可忽略的概率解决DBDH问题的有效算法，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困难问题假设下，本文的方案是EUF-IDTRSC-CMIA安全的。

证明：假设伪造者 $\mathcal{A}$ 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 $\mathcal{A}$ 解决CDH问题，从而导致矛盾。

给定B一个CDH问题的实例 (g,g^a,g^b)，它的目标是计算出 g^{ab}。为此，B模仿 $\mathcal{A}$ 的挑战者，具体过程如下：

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将公开参数发送给伪造者 $\mathcal{A}$。

询问阶段：敌手 $\mathcal{A}$ 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。

伪造阶段：敌手 $\mathcal{A}$ 输出在环成员列表 $L^*=\{ID_1^*,\cdots,$

$ID_n^*\}$、门限值 t、消息 m^* 以及门限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：

①$F(ID_i^*)=0 \bmod p$ 对于所有的 $i\in(1,\cdots,n)$ 都成立；

②$K(M^*)=0 \bmod p$，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：

$$\left(\frac{\sigma_4^*}{(\sigma_5^*)^{L(M^*)}}\right)^{1/t}=\left(\frac{g_2^{u+\sum_{i=1}^{n}r_i(U_i)}(m'\prod_{i\in\mathcal{M}}m_i)^{r_m^*}}{g^{r_m^*\cdot L(M^*)}}\right)^{1/t}$$

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

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，那么就存在一个有效的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。

3.4 方案效率

相对于群元素的点乘运算和指数运算等运算而言，双线性对计算所花费的计算成本较高，故这里只考虑双线性对运算的计算量。在本方案中，因 $z_1=e(g_1,g_2)$ 和 $z_2=e(g,g_2)$ 可以进行预计算，所以在对方案的运算量进行计算时，忽略这部分的计算量。通过对方案进行分析可知，在门限环签密产生阶段不需要双线性对计算。而在解签密阶段仅需要 3 次双线性对计算，虽然文献[15]也是在解签密阶段需要 3 次双线性对计算，然而该方案是基于随机预言模型的，相对于该方案而言，本文所提方案具有更高的安全性。

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不可伪造性，因此，本文所提方案是安全可靠的。

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signature schemes [C]// Proceedings of Crypto 1984. volume 196 of LNCS, 1984: 47-53

[2] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[C] // Proceedings of Crypto 2001. volume 2139 of LNCS, 2001: 213-229

[3] Florian Hess. Efficient identity based signature schemes based on pairings[C] // Proceedings of SAC 2002. volume 2595 of LNCS, 2002: 310-324

[4] Paterson K G, Schuldt J C N. Efficient identity-based signatures secure in the standard model[C]// Proceedings of ACISP 2006. volume 4058 of LNCS, 2006: 207-222

[5] Zheng Yu-liang. Digital signcryption or how to achieve cost(signature & encryption)≪cost(signature)+cost(encryption) [C]// Advances in Cryptology-Crypto 1997. volume 1294 of LNCS, Springer-Verlag, 1997: 165-179

[6] Duan S S, Cao Z F, Lu R X. Robust id-based threshold signcryption scheme from pairings[C]// Proceedings of the 3rd International Conference on Information Security. ACM, 2004: 33-37

[7] Peng C G, Li X. An identity-based threshold signcryption scheme with semantic security[C]// Proceedings of CIS 2005. volume 3802 of LNCS, Springer-Verlag, 2005: 173-179

[8] Li F G, Yu Y. An efficient and provably secure id-based threshold signcryption scheme[C]// Proceedings of ICCCAS 2008. IEEE Press, 2008: 488-492

[9] Zhu Z C, Zhang Y Q, Wang F J. The analysis of an efficient and provably secure id-based threshold signcryption scheme and its secure version [C] // Proceedings of the Second International Conference on Provable Security. volume 5324 of LNCS, Springer Verlag, 2008: 210-225

[10] 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]// Proceedings of the 19th International Conference on Advanced Information Networking and Application 2005. volume 2, 2005: 649-654

[11] Zhang M W, Yang B, Zhu S L, et al. Efficient secret authenticatable anonymous signcryption scheme with identity privacy[C]// Proceedings of IEEE ISI 2008. volume 5075 of LNCS, Springer-Verlag, 2008: 126-137

[12] Zhun L J, Zhang F T. Efficient id-based ring signature and ring signcryption schemes [C] // Proceedings of CIS 2008. IEEE Press, 2008: 303-307

[13] Zhu Z C, Zhang Y Q, Wang F J. An efficient and provable secure identity-based ring signcryption scheme[J]. Computer Standards & Interfaces, 2009, 31: 1092-1097

[14] Sharmila Deva Selvi S, Sree Vivek S, Pandu Rangan C. On the security of identity based ring signcryption schemes [C]// Proceedings of the 12th International Conference on Information Security. volume 5735 of LNCS, Springer-Verlag, 2009: 310-325

[15] 罗大文，何明星，李琥. 基于身份的门限环签密方案[J]. 计算机工程与应用，2011，47(33)：65-67

(上接第 130 页)

[10] Menon A, Santos J R, Turner Y, et al. Diagnosing Performance Overheads in the Xen Virtual Machine Environment[C]// Proc. of the First ACM/USENIX International Conference on Virual Execution Environments. 2005: 13-23

[11] Jin H, Deng L, Wu S, et al. Live virtual machine migration with adaptive memory compression[C]// Proc. of the 2009 IEEE International Conference on Cluster Computing (Cluster 2009). 2009

[12] Zhao W M, Wang Z L, Luo Y W. Dynamic Memory Balancing for Virtual Machines[C]// Proc. of the 2009 ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments. 2009: 37-47

[13] Du Y Y, Yu H L, Shi G G, et al. Microwiper: Efficient Memory Propagation in Live Migration of Virtual Machines[C]// Proc. of the 2010 39th International Conference on Parallel Processing. 2010: 141-149

[14] 陈阳，怀进鹏，胡春明. 基于内存混合复制方式的虚拟机在线迁移机制[J]. 计算机学报，2011，34(12)：2279-2291