标准模型下基于身份的环签密方案

孙 华[1] 郑雪峰[2] 姚宣霞[2] 刘行兵[2]

(安阳师范学院计算机与信息工程学院 安阳 455000)[1] (北京科技大学信息工程学院 北京 100083)[2]

摘 要 签密是一个同时提供认证性和保密性的密码学术语,而与分别签名和加密相比,它却具有较低的计算成本。环签密除具有签密的一般属性外还具有匿名性,它允许任一用户代表一组用户进行签密,却不知道真正是谁生成了该签密。提出了一种有效的标准模型下基于身份的环签密方案,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及在适应性选择密文攻击下的不可区分性。

关键词 环签密,标准模型,CDH问题,双线性对

中图法分类号 TP309 **文献标识码** A

Identity-based Ring Signcryption Scheme in the Standard Model

SUN Hua[1] ZHENG Xue-feng[2] YAO Xuan-xia[2] LIU Xing-bing[2]

(School of Computer and Information Engineering, Anyang Normal University, Anyang 455000, China)[1]

(School of Information Engineering, University of Science and Technology Beijing, Beijing 100083, China)[2]

Abstract Signcryption is a cryptographic primitive which provides authentication and confidentiality simultaneously with a computational cost lower than signing and encryption respectively. The ring signcryption has anonymity in addition to authentication and confidentiality, which allows any user to choose any set of users that includes himself and signcrypt messages without revealing who in the set has actually produced it. This paper presented an efficient identity-based ring signcryption scheme in the standard model, which proves its indistinguishability against adaptive chosen ciphertext attacks and existential unforgeability against adaptive chosen message and identity attacks in terms of the hardness of CDH problem and DBDH problem.

Keywords Ring signcryption, Standard model, Computational Diffie-Hellman problem, Bilinear pairing

1984年,Shamir[1]提出了基于身份的密码体制,用以消除公钥PKI体制中的证书管理。在基于身份的密码系统中,用户的公钥由用户的唯一身份信息计算得到,而其私钥则由PKG利用主密钥生成。

匿名性是密码学应用的一个重要属性。在实际的应用中,例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[2]首先由Rivest等人提出。它由某一用户代表群用户生成,验证者可以对它进行验证却不知道真正的签名者是谁,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[3-5]被相继提出。不同于群签名[6,7],环签名中群的形成是自发的,不需要有群管理者;签名者只要简单地选取群成员的公钥和自己的私钥,就可以生成环签名。这种签名方法可以极大地降低相互认证的复杂性,同时提供签名者的匿名性。

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[8]首次提出了签密的概念,即能够在一个合理的步骤内同时完成加密和数字签名两项功能,而其通信成本和计算量都低于传统的先签名后加密方法。2002年,Malone-Lee[9]提出了第一个基于身份的签密方案,后来一些签密方案[10,11]被相继提出。

Huang等人[12]首先提出了环签密的方案,然而该方案是计算低效的。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。目前已有的环签密方案大多是在随机预言模型下证明安全的,然而,在具体应用中有时却无法构造相应的实例。因此,在标准模型下设计可证安全的基于身份的环签密方案更具有实际意义。

1 预备知识

1.1 双线性对

设G,G_T是两个阶为素数q的循环群,g是群G的生成元,双线性对$e:G\times G\rightarrow G_T$是具有如下性质的映射:

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

到稿日期:2009-10-26 返修日期:2010-01-19 本文受国家自然科学基金项目(No. 60674054)资助。

孙 华(1980-),男,博士,主要研究方向为密码学与信息安全,E-mail:sh1227@163.com;郑雪峰(1951-),男,教授,博士生导师,主要研究方向为信息安全技术;姚宣霞(1973-),女,博士生,副教授,主要研究方向为无线传感器网络及信息安全;刘行兵(1972-),男,博士生,讲师,主要研究方向为信息安全与密码学。

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 $P,Q\in G$。

1.2 相关困难问题

定义 1 给定群 G 的生成元 P，元组 (P^a,P^b,P^c)，$h\in G_T$，$a,b,c\in Z_q^*$，则 DBDH 问题为：判定是否 $h=e(P,P)^{abc}$。

我们定义敌手解决 DBDH 问题的优势为：

$$Adv_{\mathscr{A}}^{DBDH}=|Pr[\mathscr{A}(P^a,P^b,P^c,e(P,P)^{abc})=1]-Pr[\mathscr{A}(P^a,P^b,P^c,h)=1]|$$

定义 2 给定群 G 的生成元 P，元组 (P^a,P^b)，$a,b\in Z_q^*$，则 CDH 问题为：计算 P^{ab}。

我们定义敌手解决 CDH 问题的优势为：

$$Adv_{\mathscr{A}}^{CDH}=Pr[\mathscr{A}(P,P^a,P^b)=P^{ab}]$$

2 基于身份的环签密

2.1 形式化定义

一个基于身份的环签密方案由以下 4 个算法组成。

1. Setup：给定安全参数 k，PKG 生成系统公开参数 *params*、公钥 P_{pub} 以及主密钥 *msk*。

2. Extract：给定身份 *ID*，PKG 计算 *ID* 的相应私钥 S_{ID}，并秘密发送给它。

3. Signcrypt：给定消息 m、接收者身份 ID_R、签密者的私钥 D_S 以及环成员组 $\{ID_1,\cdots,ID_n\}$，该算法生成密文 C。

4. Unsigncrypt：该算法输入密文 C、接收者的私钥 D_R、环成员的身份 $\{ID_1,\cdots,ID_n\}$，如果 C 是一个有效的密文，则生成明文 m，否则输出 $\perp$。

2.2 IDRSC 安全模型

定义 3 一个基于身份的环签密方案在适应性选择密文的攻击下是不可区分的(IND-IDRSC-CCA)，如果没有概率多项式时间的敌手 $\mathscr{A}$，在下面的游戏中可获得不可忽略的优势：

Setup：挑战者 $\mathscr{C}$ 运行 Setup 算法生成系统参数 *params* 并发送给敌手 $\mathscr{A}$，保存主密钥 *msk*。

First Phase：敌手 $\mathscr{A}$ 可以适应性地向挑战者 $\mathscr{C}$ 发出如下一定数量的询问：

Extract query：$\mathscr{A}$ 选择身份 *ID*，$\mathscr{C}$ 计算其私钥 D_S 并发送给 $\mathscr{A}$。

Signcrypt query：$\mathscr{A}$ 选择签密者 ID_S、环成员组 U、接收者 ID_R 及明文 m。$\mathscr{C}$ 运行 Extract 算法得到 ID_S 的私钥 D_S，然后运行 Signcrypt 算法生成密文 C 并发送给 $\mathscr{A}$。

Unsigncrypt query：$\mathscr{A}$ 选择环成员组 U、接收者 ID_R 和密文 C。$\mathscr{C}$ 运行 Extract 算法得到 ID_R 的私钥 D_R，如果 $\mathscr{C}$ 是一个有效的密文，则运行算法 Unsigncrypt 返回 m，否则，返回 $\perp$。

Challenge：$\mathscr{A}$ 任选两个相同长度的消息 m_0、m_1、环成员组 U 以及挑战身份 ID_R。$\mathscr{A}$ 不能在第一阶段中询问 U 中任一成员及 ID_R 的私钥。$\mathscr{C}$ 选一位 $b\in\{0,1\}$，计算 m_b 的签密 C^*，并将其发送给 $\mathscr{A}$。

Second Phase：$\mathscr{A}$ 可以像步骤 2 那样发起一定数量的任意询问，但不能对 U 中任一成员及 ID_R 的私钥发起询问，同时不能对 C^* 发起 Unsigncrypt 询问。

Guess：$\mathscr{A}$ 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 $Succ_{\mathscr{A}}^{IND-IDRSC-CCA}=2Pr[b=b']-1$。

定义 4 一个基于身份的环签密方案在适应性选择消息和身份攻击下可抵抗存在性伪造(EUF-IDRSC-CMIA)，如果没有概率多项式时间的敌手 $\mathscr{A}$，在下面的游戏中可获得不可忽略的优势：

Setup：挑战者 $\mathscr{C}$ 运行 Setup 算法生成系统参数 *params* 并发送给敌手 $\mathscr{A}$，保存主密钥 *msk*。

Query：$\mathscr{A}$ 可以像定义 3 中的第一阶段那样，发起一定数量的任意询问。

Forgery：$\mathscr{A}$ 输出新元组 (U,ID_R,C)，其中 U 中任一成员及 ID_R 的私钥没有询问过。如果 $Uusigncrypt(U,D_R,C)$ 的结果不为 $\perp$，那么 $\mathscr{A}$ 赢得游戏。如果 $\mathscr{A}$ 能够生成有效的签密，则 $\mathscr{C}$ 可以解决 CDH 问题。

3 标准模型下基于身份的环签密方案

3.1 方案描述

令 G 和 G_T 是两个阶为素数 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 $H_1:\{0,1\}^*\to\{0,1\}^{n_u}$ 和 $H_2:\{0,1\}^*\to\{0,1\}^{n_m}$ 将任意长度的身份 *ID* 和消息 m 输出为长度为 n_u 和 n_m 的位串，方案由如下算法构成：

系统建立：随机选取 $\alpha\in Z_p$，G 的任意生成元 g，计算 $g_1=g^\alpha$。随机选取 $g_2,u',m'\in G$，向量 $\hat{U}=(\hat{u}_1,\hat{u}_2,\cdots,\hat{u}_{n_u})\in G^{n_u}$，向量 $\hat{M}=(\hat{m}_1,\hat{m}_2,\cdots,\hat{m}_{n_m})\in G^{n_m}$。公开参数为 $params=(G,G_T,e,g,g_1,g_2,u',\hat{U},m',\hat{M})$，主密钥为 $msk=g_2^\alpha$。

密钥生成：令 $u_s=H_1(ID_s)$ 为身份 ID_s 的长为 n_u 的位串，$u[i]$ 表示 u_s 中的第 i 位，$u_s\subseteq\{1,2,\cdots,n_u\}$ 表示 $u[i]=1$ 的序号 i 的集合，任选 $r_{u_s}\in Z_p$，则身份 ID_s 的私钥为：

$$d_{ID_s}=(d_{s1},d_{s2})=(g_2^\alpha(u'\prod_{i\in u_s}\hat{u}_i)^{r_{u_s}},g^{r_{u_s}})$$

签密：令 $U=\{ID_1,\cdots,ID_n\}$ 为环签密中 n 个成员的集合，计算 $m=H_2(m,U)$，$\Omega\subseteq\{1,2,\cdots,n_m\}$ 为消息 m 的位串中第 j 位 $m[j]=1$ 的序号 j 的集合，$u_j=u'\prod\hat{u}_i$，$i\in u_j$，$j=1,\cdots,n$，$\mathscr{M}=m'\prod_{i\in\Omega}\hat{m}_i$。设签密者的身份为 ID_π，$\pi\in[1,n]$，其私钥为 $d_{ID_\pi}=(d_{\pi1},d_{\pi2})$，签密接收者的身份为 ID_k。随机选取 $r_1,\cdots,r_n,r_m\in Z_P$，计算 $R_i=g^{r_i}$，$i=1,\cdots,n$，$i\neq\pi$，$R_\pi=d_{\pi2}g^{r_\pi}$，$R_m=g^{r_m}$。令 $C_1=g^{r_\pi}$，$C_2=(U_k)^{r_\pi}$，$C_3=d_{\pi1}\prod_{i=1}^{n}(U_i)^{r_i}(\mathscr{M})^{r_m}$，$C_4=e(g_1,g_2)^{r_\pi}\oplus\langle m,ID_\pi,C_3,R_1,\cdots,R_n,R_m\rangle$，则生成的密文为 $\sigma=(C_1,C_2,C_3,C_4,R_1,\cdots,R_n,R_m)$。

解密：当收到签密 σ 后，接收者 ID_k 进行如下计算：

1)由接收者 ID_k 的私钥 $d_{ID_k}=(d_{k1},d_{k2})$ 计算 $W=e(C_1,d_{k1})\cdot e(d_{k2},C_2)^{-1}$。

2)由 $\langle m,ID_\pi,C_3,R_1,\cdots,R_n,R_m\rangle=C_4\oplus W$ 及环成员组 $U=\{ID_1,\cdots,ID_n\}$，计算 $m=H_2(m,U)$，$u_j=u'\prod\hat{u}_i$，$i\in u_j$，$j=1,\cdots,n$，$\mathscr{M}=m'\prod_{i\in\Omega}\hat{m}_i$，当且仅当等式 $e(C_3,g)=e(g_1,g_2)\cdot\prod_{i=1}^{n}e(U_i,R_i)\cdot e(\mathscr{M},R_m)$ 成立时，σ 为一个有效的环签密。

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：

由 $d_{ID_k}=(d_{k1},d_{k2})=(g_2^\alpha(u'\prod_{i\in u_k}\hat{u}_i)^{r_{u_k}},g^{r_{u_k}})$ 可得：

$$W=e(C_1,d_{k1})\cdot e(d_{k2},C_2)^{-1}=e(g^{r_\pi},g_2^a(U_k)^{r_{u_k}})\cdot e(g^{r_{u_k}},(U_k)^{r_\pi})^{-1}=\frac{e(g^{r_\pi},g_2^a)\cdot e(g^{r_\pi},(U_k)^{r_{u_k}})}{e(g^{r_{u_k}},(U_k)^{r_\pi})}$$

$$=e(g_1,g_2)^{r_\pi}$$

对 σ 进行验证可得：

$$e(C_3,g)=e(g_2^a(U_\pi)^{r_{u_\pi}}(U_1)^{r_1}\cdots(U_n)^{r_n}(\mathcal{M})^{r_m},g)$$

$$=e(g_2^a(U_1)^{r_1}\cdots(U_\pi)^{r_{u_\pi}+r_\pi}\cdots(U_n)^{r_n}(\mathcal{M})^{r_m},g)$$

$$=e(g_1,g_2)e(U_1,g)^{r_1}\cdots e(U_n,g)^{r_n}e(\mathcal{M},g)^{r_m}$$

$$=e(g_1,g_2)e(U_1,R_1)\cdots e(U_n,R_n)e(\mathcal{M},R_m)$$

3.3 方案安全性

定理 1 如果我们的方案是 $(\varepsilon,t,q_e,q_s,q_u)$-EU-IDRSC-CMIA 安全的，即不存在运行时间至多为 t、优势为 ε 的敌手 $\mathcal{A}$，并且其私钥询问的次数最多为 q_e，签密询问的次数最多为 q_s，解密询问的次数最多为 q_u，在 CDH 困难问题假设下，我们可以概率 $\varepsilon'\geqslant\frac{\varepsilon}{2^{n+3}q_s(q_e+q_s)^n(n_u+1)^n(n_m+1)}$ 解决 CDH 问题，其运行时间为 $t+O((q_en_u+q_s(nn_u+n_u+n_m))\rho+(q_e+nq_s)\tau+q_s\tau')$，$\rho$ 和 τ 分别为 G 中一次乘法运算和指数运算的时间，τ' 为 G_T 中一次指数运算的时间。

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。

给定 B 一个 CDH 问题的实例 (g,g^a,g^b)，为了计算 g^{ab}，B 模仿 $\mathcal{A}$ 的挑战者，具体过程如下：

Setup　令 $l_u=2(q_e+q_s)$，$l_m=2q_s$。B 随机选择 k_u,k_m，满足 $0\leqslant k_u\leqslant n_u$，$0\leqslant k_m\leqslant n_m$，并假定 $l_u(n_u+1)<p$，$l_m(n_m+1)<p$。选择 $x'\in_R Z_{l_u}$ 及长度为 n_u 的向量 $X=(x_i)$，其中 $x_i\in_R Z_{l_u}$；B 又选择 $z'\in_R Z_{l_m}$ 及长度为 n_m 的向量 $Z=(z_j)$，其中 $z_j\in_R Z_{l_m}$。最后 B 选择 $y',w'\in_R Z_p$ 和长度为 n_u 的向量 $Y=(y_i)$ 及长度为 n_m 的向量 $W=(w_j)$，其中 $y_i,w_j\in_R Z_p$。

对环成员组 U 中任一成员身份 ID 和消息 m 来说，令 $H_1(ID)\to u$，$H_2(m,U)\to m$，定义

$$F(u)=(p-l_uk_u)+x'+\sum_{i\in u}x_i,J(u)=y'+\sum_{i\in u}y_i$$

$$K(m)=(p-l_mk_m)+z_j'+\sum_{j\in\Omega}z_j,L(m)=w'+\sum_{j\in\Omega}w_j$$

算法 B 构造上面方案中的公开参数如下：

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

$$u'=g_2^{p-l_uk_u+x'}g^{y'},\hat{u}_i=g_2^{x_i}g^{y_i},1\leqslant i\leqslant n_u$$

$$m'=g_2^{p-l_mk_m+z'}g^{w'},\hat{m}_j=g_2^{z_j}g^{w_j},1\leqslant j\leqslant n_m$$

可以看出这些参数的分布与一个真正的挑战者所产生公开参数的分布是一样的，且对任何身份 ID_u 及消息 m，我们有等式：

$$u'\prod_{i\in u_u}\hat{u}_i=g_2^{F(u_u)}g^{J(u_u)},m'\prod_{j\in\Omega}\hat{m}_j=g_2^{K(m)}g^{L(m)}$$

然后算法 B 将公开参数发送给敌手 $\mathcal{A}$。

Oracles Simulation：B 将按如下方式模仿 $\mathcal{A}$ 对挑战者的询问：

①Extract oracle：当敌手 $\mathcal{A}$ 问身份 ID_j 的私钥时，B 首先计算 $u_j=H_1(ID_j)$。虽然算法 B 不知道主密钥，但假定 $F(u_j)\neq 0 \bmod p$，B 也能够构造其私钥 d_{ID_j}。B 任选 $r_{u_j}\in Z_p$ 并计算：

$$d_{ID_j}=(d_{j1},d_{j2})=(g_1^{-J(u_j)/F(u_j)}(u'\prod_{i\in u_j}\hat{u}_i)^{r_{u_j}},g_1^{-1/F(u_j)}g^{r_{u_j}})$$

令 $\tilde{r}_{u_j}=r_{u_j}-a/F(u_j)$，可以验证 d_{ID_j} 是 ID_j 的有效私钥。

$$d_{j1}=g_1^{-J(u_j)/F(u_j)}(u'\prod_{i\in U_j}\hat{u}_i)^{r_{u_j}}$$

$$=g_2^a(g_2^{F(u_j)}g^{J(u_j)})^{-a/F(u_j)}(g_2^{F(u_j)}g^{J(u_j)})^{r_{u_j}}$$

$$=g_2^a(g_2^{F(u_j)}g^{J(u_j)})^{r_{u_j}-a/F(u_j)}$$

$$=g_2^a(u'\prod_{i\in U_j}\hat{u}_i)^{\tilde{r}_{u_j}}$$

$$d_{j2}=g_1^{-1/F(u_j)}g^{r_{u_j}}=g^{r_{u_j}-a/F(u_j)}=g^{\tilde{r}_{u_j}}$$

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

②Signcrypt oracle：在任何时候，$\mathcal{A}$ 都可以发起在环成员组 U 和接收者 ID_R 下对消息 m 的签密询问。如果对某个 $ID_S\in U$，我们有 $F(u_s)\neq 0 \bmod p$，则 B 首先运行密钥生成算法得到 ID_S 的私钥 D_S，然后运行签密算法 Signcrypt(m,U,D_S,ID_R) 生成一个有效的签密 σ 并发送给 $\mathcal{A}$。如果对所有 $ID_S\in U$，都有 $F(u_s)=0 \bmod p$，B 可以采用与构造私钥相同的方法构造一个有效的签密。假定 $K(m)\neq 0 \bmod p$，随机选取 $r_1,\cdots,r_n$，$r_m\in Z_p$ 和签密者 ID_π，计算 $R_i=g^{r_i}$，$i=1,\cdots,n$，$R_m=g_1^{-1/K(m)}g^{r_m}$，$C_1=g^{r_\pi}$，$C_2=(U_k)^{r_\pi}$，$C_3=g_1^{-\frac{L(m)}{K(m)}}\prod_{i=1}^{n}(U_i)^{r_i}(\mathcal{M})^{r_m}$，$C_4=e(g_1,g_2)^{r_\pi}\oplus\langle m,ID_\pi,C_3,R_1,\cdots,R_n,R_m\rangle$，则生成的密文为 $\sigma=(C_1,C_2,C_3,C_4,R_1,\cdots,R_n,R_m)$。

③Unsigncrypt oracle：在任何时候，$\mathcal{A}$ 都可以发起在环成员组 U 和接收者 ID_R 下对密文 σ 的解密询问。如果 $F(u_r)\neq 0 \bmod p$，B 首先运行密钥生成算法得到 ID_R 的私钥 D_R，然后运行解密算法 Unsigncrypt(σ,U,D_R) 将结果发送给 $\mathcal{A}$；否则，B 将失败退出。

在 $\mathcal{A}$ 发出一定数量的私钥询问、签密询问以及解密询问后，如果整个过程中 B 没有失败退出，那么 $\mathcal{A}$ 可以输出一个在环成员组 U^* 和接收者 ID_R^* 下对消息 m^* 的有效伪造签密 σ^*。如果有 $F(u_i^*)=0 \bmod p$，$1\leqslant i\leqslant n$ 且 $K(m^*)=0 \bmod p$，其中 $u_i^*=H_1(ID_i^*)$，则可得：

$$\frac{C_3^*}{R_1^{*J(u_1^*)}\cdots R_n^{*J(u_n^*)}R_m^{*L(m^*)}}=\frac{g_2^a(U_1)^{r_1}\cdots(U_n)^{r_n}(M)^{r_m}}{g^{J(u_1^*)r_1}\cdots g^{J(u_n^*)r_n}g^{L(m^*)r_m}}$$

$$=\frac{g_2^a(g_2^{F(u_1^*)}g^{J(u_1^*)})^{r_1}\cdots(g_2^{F(u_n^*)}g^{J(u_n^*)})^{r_n}(g_2^{K(m^*)}g^{L(m^*)})^{r_m}}{g^{J(u_1^*)r_1}\cdots g^{J(u_n^*)r_n}g^{L(m^*)r_m}}$$

$$=g_2^a=g^{ab}$$

这就是 CDH 问题实例的解，否则，B 将失败退出。

下面分析算法 B 成功的概率。

如果算法 B 在整个过程中没有失败退出，那么需要满足以下 3 个条件：

1. 对身份 ID 进行私钥询问时，有 $F(u)\neq 0 \bmod l_u$，$u=H_1(ID)$。

2. 对 (U,m) 进行签密询问时，或者对某个 $i\in n$，有 $F(u_i)\neq 0 \bmod l_u$，或者 $K(m)\neq 0 \bmod l_m$，$m=H_2(m,U)$。

3. 对所有 $j\in n$，有 $F(u_j^*)\neq 0 \bmod l_u$ 且 $K(m^*)=0 \bmod l_m$。

令 q_I 为私钥询问和签密询问中进行 H_1 询问的次数，其中不包括对 U^* 中身份的询问，q_M 为包括挑战身份 U^* 下在签密询问中进行 H_2 询问的次数。我们有 $q_I\leqslant q_e+q_s$，$q_M\leqslant q_s$。定义事件 A_i,A^*,B_k,B^* 如下：

$A_i:F(u_i)\neq 0 \bmod l_u$，$A^*:F(u^*)=0 \bmod p$

$B_k:K(m_k)\neq 0 \bmod l_m$，$B^*:K(m^*)=0 \bmod p$

那么 B 不失败退出的概率为：

$$P_r[\neg abort]\geqslant P_r[\bigwedge_{i=1}^{q_I} A_i \wedge A^* \wedge \bigwedge_{k=1}^{q_M} B_k \wedge B^*]$$

由于事件 A_i, A^*, B_k, B^* 是相互独立的，且由假设 $l_u(n_u+1)<p$ 可知，如果 $F(u)=0 \bmod p$，则有 $F(u)=0 \bmod l_u$，因此

$$P_r[A^*]=\prod_{j=1}^{n} P_r[F(u_j^*)=0 \bmod p \wedge F(u_j^*)=0 \bmod l_u]$$

$$=\prod_{j=1}^{n} P_r[F(u_j^*)=0 \bmod l_u]P_r[F(u_j^*)=0 \bmod p \mid F(u_j^*)=0 \bmod l_u]=[\frac{1}{l_u(n_u+1)}]^n$$

另一方面，我们有 $P_r[\bigwedge_{i=1}^{q_I} A_i \mid A^*]=1-P_r[\bigvee_{i=1}^{q_I} \overline{A_i} \mid A^*]\geqslant 1-\sum_{i=1}^{q_I} P_r[\overline{A_i} \mid A^*]$，由 $P_r[\overline{A_i} \mid A^*]=1/l_u$ 及 $l_u=2(q_e+q_s)$，我们可得：

$$P_r[\bigwedge_{i=1}^{q_I} A_i \wedge A^*]=P_r[A^*]P_r[\bigwedge_{i=1}^{q_I} A_i \mid A^*]$$

$$=\left[\frac{1}{l_u(n_u+1)}\right]^n(1-\frac{q_I}{l_u})$$

$$\geqslant\left[\frac{1}{l_u(n_u+1)}\right]^n(1-\frac{q_e+q_s}{l_u})$$

$$=\frac{1}{2^{n+1}(q_s+q_e)^n(n_u+1)}$$

类似地，可以得到：

$$P_r[\bigwedge_{k=1}^{q_M} B_k \wedge B^*]\geqslant\frac{1}{4q_s(n_m+1)}$$

综合上面的结果，可得：

$$P_r[\neg abort]\geqslant\frac{1}{2^{n+3}q_s(q_e+q_s)^n(n_u+1)^n(n_m+1)}$$

如果 $\mathcal{A}$ 以不可忽略的概率 ε 生成一个伪造签密，B 在整个模拟过程中没有失败退出，那么 B 可以概率 $\varepsilon'\geqslant\frac{\varepsilon}{2^{n+3}q_s(q_e+q_s)^n(n_u+1)^n(n_m+1)}$ 解决 CDH 问题的实例。

时间复杂度分析：私钥询问需要 $O(n_u)$ 次 G 中乘法运算和 $O(1)$ 次指数运算，签密询问需要 $O(nn_u+n_u+n_m)$ 次 G 中乘法运算和 $O(n)$ 次指数运算及 $O(1)$ 次 G_T 中指数运算，故总的时间为 $t+O((q_en_u+q_s(nn_u+n_u+n_m))\rho+(q_e+nq_s)\tau+q_s\tau')$。

定理 2 在 DBDH 困难问题的假设下，我们的方案是 IND-IDRSC-CCA 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。

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有 $h=e(g,g)^{abc}$。B 模仿 $\mathcal{A}$ 的挑战者，其过程如下：

Setup 构造与前面证明中相同的系统公开参数，并把它们发送给 $\mathcal{A}$。

Phase 1 敌手 $\mathcal{A}$ 可如同前面证明那样，适应性发起一定数量的私钥询问、签密询问及解密询问。

Challenge 在第一阶段后，$\mathcal{A}$ 任取两个相同长度的消息 m_0, m_1，发起挑战的环成员组 $U=\{ID_1, \cdots, ID_n\}$ 和接收者 ID_R 并发送给 B。如果 $\mathcal{A}$ 在第一阶段询问了 U 中任一成员或 ID_R 的私钥，B 将失败退出。B 任选一位 $b\in\{0,1\}$，如果 $K(m_b)\neq 0 \bmod p, F(u_r)\neq 0 \bmod p$，那么 B 将失败退出。否则，B 任选签密者 ID_S，随机选取 $r_1, \cdots, r_n, r_m\in\mathbb{Z}_p$，令 $u_k=H_1(ID_k), 1\leqslant k\leqslant n, \tilde{r}_s=r_s-a/F(u_s), m_b=H_2(m_b, U)$。构造 $R_i=g^{r_i}, i=1,\cdots,n, R_m=g^{r_m}, C_1=g^c, C_2=g^{cJ(u_r)}, C_3=g_1^{\frac{-J(u_s)}{F(u_s)}}\prod_{i=1}^{n}(U_i)^{r_i}g^{r_mL(m_b)}, C_4=h\oplus\langle m_b, ID_S, C_3, R_1, \cdots, R_n, R_m\rangle$。

如果 $h=e(g,g)^{abc}$，由 $F(u_r)=0 \bmod p, K(m_b)=0 \bmod p, u'\prod_{i\in u_r}u_i=g_2^{F(u_r)}g^{J(u_r)}, m'\prod_{j\in\Omega_b}m_j=g_2^{K(m_b)}g^{L(m_b)}$，可得：

$$C_1=g^c$$

$$C_2=g^{cJ(u_r)}=(g_2^{F(u_r)}g^{J(u_r)})^c=(u'\prod_{i\in u_r}\hat{u}_i)^2$$

$$C_3=g_1^{\frac{-J(u_s)}{F(u_s)}}\prod_{i=1}^{n}(U_i)^{r_i}g^{r_mL(m_b)}$$

$$=g_1^{\frac{-J(u_s)}{F(u_s)}}\prod_{i=1}^{n}(g_2^{F(u_i)}g^{J(u_i)})^{r_i}g_2^{r_mK(m_b)}g^{r_mL(m_b)}$$

$$=g_2^{a}\prod_{k=1,k\neq s}^{n}(u'\prod_{i\in u_k}\hat{u}_i)^{r_k}(u'\prod_{i\in u_s}\hat{u}_i)^{\tilde{r}_s}(m'\prod_{j\in\Omega_b}\hat{m}_j)^{r_m}$$

$$C_4=h\oplus\langle m_b, ID_S, C_3, R_1, \cdots, R_n, R_m\rangle$$

$$=e(g_1,g_2)^c\oplus\langle m_b, ID_S, C_3, R_1, \cdots, R_n, R_m\rangle$$

$$\sigma=(C_1, C_2, C_3, C_4, R_1, \cdots, R_n, R_m)$$

可知 σ 是一个有效的环签密。

Phase 2 敌手 $\mathcal{A}$ 可以如同阶段 1 那样，发出一定数量的私钥询问、环签密询问及解密询问，但是 $\mathcal{A}$ 不能询问 ID_R 的私钥以及对 σ 的解密询问。

Guess 最后，$\mathcal{A}$ 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，如果存在一个敌手以不可忽略的概率进行 CCA 攻击，那么就存在一个有效的算法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-IDRSC-CCA 安全的。

结束语 本文提出了一种有效的标准模型下可证明安全的基于身份环签密方案，并给出了相应的安全模型。它不仅具有签密的一般属性，而且具有匿名性。最后，我们利用 DBDH 问题的困难性证明了方案的不可区分性，同时利用 CDH 问题的困难性证明了方案的不可伪造性，并对方案进行了概率分析和时间复杂度分析。

参 考 文 献

[1] Shamir A. Identity-based Cryptosystems and Signature Schemes [C]// Proceedings of Crypto 1984, volume 196 of LNCS. Springer-Verlag, 1985: 47-53

[2] Rivest R L, Shamir A, Tauman Y. How to Leak a Secret[C]// Proceedings of Asiacrypt 2001, volume 2248 of LNCS. Springer-Verlag, 2001: 552-565

[3] Chow S S L, Yiu S M, Hui L C K. Efficient Identity Based Ring Signature[C] // Applied Cryptography and Network Security 2005, volume 3531 of LNCS. Springer-Verlag, 2005: 499-512

[4] Xu Jing, Zhang Zhen-feng, Feng Deng-guo. A Ring Signature Scheme Using Bilinear Pairings[C]// WISA 2004, volume 3325 of LNCS. Springer-Verlag, 2005: 160-169

[5] Au M H, Liu J K, Yuen T H, et al. ID-based Ring Signature Scheme Secure in the Standard Model[C]// IWSEC 2006, volume 4266 of LNCS. Springer-Verlag, 2006: 1-16

[6] Camenisch J, Stadler M. Efficient Group Signature Schemes for Large Groups(extended abstract)[C]// Advances in CRYPTO' 97, volume 1294 of LNCS. Springer-Verlag, 1997: 410-424

[7] Bellare M, Micciancio D, Warinschi B. Foundations of Group Signatures: Formal Definitions, Simplified Requirements and a

Construction Based on General Assumptions[C]// EUROCRYPT'03, volume 2656 of LNCS. Springer-Verlag, 2003: 614-629

[8] 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

[9] Lee J M. Identity-based Signcryption[R]. Report 2002/098. Cryptology ePrint Archive, 2002. http://eprint.iacr.org/

[10] Libert B, Quisquater J J. New Identity Based Signcryption Schemes from Pairings[R]. Report 2003/023. Cryptology ePrint Archive, 2003. http://eprint.iacr.org/

[11] Peng Chang-gen, Li Xiang. An Identity-based Threshold Signcryption Scheme with Semantic Security[C]// Proceedings of CIS 2005, volume 3802 of LNCS. Springer-Verlag, 2005: 173-179

[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]// Advanced Information Networking and Application 2005. 2005, 2: 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: 670-674

[14] Li Fa-gen, Shirase M, Takagi T. Analysis and Improvement of Authenticatable Ring Signcryjption Scheme[J]. Journal of Shanghai Jiaotong University(Science), 2008, 13: 679-683

(上接第 56 页)

4.2 认知电台数量的选择

为了区别各个认知电台接收到信噪比的不同，我们选择了 3 种方案，为了保证公平性，假设各方案中系统的最大信噪比值 SNR_{max} 相同，系统的平均感知信噪比 $\overline{SNR}$ 相同，N 代表参与感知的认知无线电台数量。

方案 1: $SNR(i)=\overline{SNR}$;

方案 2: $SNR(i)=SNR_{max}-(SNR_{max}-\overline{SNR})\frac{2i}{N-1}$;

方案 3: $SNR(i)=SNR_{max}-(SNR_{max}-\overline{SNR})\frac{6i^2}{(N-1)(2N-1)}$。

从图 4 可以看到，假如认知无线电台接收到的平均感知信噪比为 $\overline{SNR}$，假设系统的探测概率应满足 $P_d\geqslant 0.9$，系统取得最佳探测性能的方案是性噪比方差大的方案 3，它可以在选择认知电台的数量最少的情况下，通过选择信噪比大的认知电台，达到系统要求的性能。

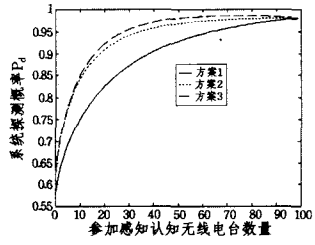

图 4 不同信噪比方案下感知电台数量与系统性能的关系

4.3 系统感知开销比较

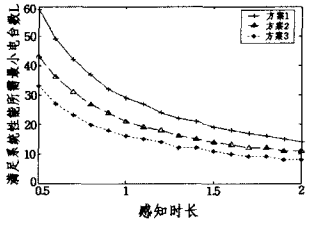

图 5 感知时长和系统所需最小电台间关系

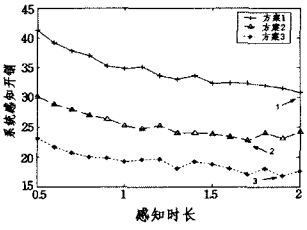

图 6 感知时长和系统开销关系

从图 5 中可以看到随着感知时间的延长，满足系统性能所需要的电台数是逐渐减少的，这是因为延长感知时间意味着认知电台相应探测性能的升高，所以所需的最小电台数是逐渐减小的。从图 6 中可以看到，系统的感知开销有最小值，对应的数值用箭头示出，相应的方案用箭头旁标号示出。以方案 2 为例，此时所需的最小感知电台数量为 15，其最佳感知时长约为 1.7ms。仿真证明了算法的正确性和有效性。

结束语 本文中，鉴于每个认知无线电台上信噪比的不同性，我们证明当电台数目无限大时，只要满足一定条件，系统的探测概率 $P_d=1$，虚警概率 $P_f=0$。如果电台数目有限时，选择全部电台参与感知并不能使系统最优，而是应该选择其中信噪比更高的部分电台参与感知，并给出满足系统性能所需的最小电台数的表达式。在此基础上，在最小化系统感知开销约束条件下，推导出其所需感知时长的条件。仿真结果说明，在认知无线电台接收到的平均感知信噪比 $\overline{SNR}$ 相同的情况下，如果选用部分性能较好的用户，则有对应的最小所需感知电台数量和相应的感知时长，使系统感知开销最小。

参 考 文 献

[1] FCC. Spectrum Policy Task Force Report, ET Docket[R]. No. 02-155. Nov. 2002

[2] Mitola J, Maquire G Q Jr. Cognitive Radio: Making Software Radios More Personal[J]. IEEE Personal Communications, 1999, 6(4): 13-18

[3] Mishra S M, Sahai A, Broderson R W. Cooperative sensing among cognitive radios[C]// Proc. IEEE International Conference on Comunications(ICC) 2006. Istanbul, Turkey, June 2006

[4] Cabric D, Mishra S M, Brodersen R W. Implementation issues in spectrum sensing for cognitive radios[C]// Proc. 38th Asilomar Conference on Signals, Systems and Computers 2004. November 2004: 772-776

[5] Liang Y-C, Peh E. Optimization for cooperative sensing in cognitive radio networks[C]// Proc. IEEE WCNC 2007. Hong Kong, China, Mar. 2007: 27-32

[6] Zhang Wei, Mallik R K, Letaief B K. Cooperative Spectrum Sensing Optimization in Cognitive Radio Networks[C]// Proc. IEEE International Conference oniee Department of ECE. Hong Kong University of Science: 3411-3415

[7] Fodor V, Glaropoulos I, Pescosolido L. Detecting low-power primary signals via distributed sensing to support opportunistic spectrum access[C]// Proccedings of IEEE ICC'09. Germany, 2009

[8] Kostylev V I. Energy detection of a signal with random amplitude[C]// Proc. IEEE Int. Conf. Commun. May 2002: 1606-1610

[9] Niu Ruixin, Varshney P K. Performance Analysis of Distributed Detection in a Random Sensor Field[J]. IEEE Transactions on Signal Processing, 2008, 56(1): 339-349