安全加密的环签名混淆器*

陈兴发[1]，高崇志[2]，姚正安[1]
（1. 中山大学数学与计算科学学院，广东 广州 510275；
2. 广州大学计算机科学与教育软件学院，广东 广州 510006）

摘 要：构造了一个安全的混淆器来实现对特殊的加密的环签名功能的混淆。这个特殊的加密的环签名功能是由 waters 的环签名方案和线性加密方案组合实现的。在标准模型下，构造的混淆器满足有关联预言的平均情况虚拟黑盒性质（ACVBP w. r. t. dependent oracles）。有了这个性质，即使敌手在获得混淆后的具有加密的环签名功能程序，环签名依然是匿名的和不可伪造的。

关键词：虚拟黑盒性质；混淆器；环签名
中图分类号：TN918 **文献标志码**：A **文章编号**：0529－6579（2014）01－0008－10

Secure Obfuscation for Encrypted Ring Signatures

CHEN Xingfa[1], *GAO Chongzhi*[2], *YAO Zhengan*[1]
(1. School of Mathematics & Computational Science, Sun Yat-sen University, Guangzhou 510275, China;
2. School of Computer Science and Educational Software, Guangzhou University, Guangzhou 510006, China)

Abstract: A concrete implementation of a secure obfuscator for a special encrypted ring signature (ERS) functionality is constructed. This ERS functionality is the sequential composition of Waters's ring signature scheme and linear encryption scheme. In the standard model, the proposed obfuscator satisfies average-case virtual black-box property (ACVBP), which guarantees the preservation of the anonymity and unforgeability of the ring signature even if an obfuscated program is given to the adversaries.

Key words: virtual black-box property; obfuscation; ring signature

Hada[1]构造了一个安全的混淆器来实现对签名后再加密的功能的混淆，使得在生成这个加密的签名的过程中没有泄露生成签名的私钥的信息。简略地说，混淆器的目的是将一段程序转换成一段外人无法了解其内部工作原理的新程序，同时这个新程序在功能上和原来的程序是一致的。一个安全的混淆器应该满足虚拟黑盒性质（virtual black-box property），简称 VBP。VBP 是指任何可以从混淆以后的程序里在多项式时间内计算出来的信息，均可以通过黑盒访问的方式访问原来的程序得到。如果存在这样安全的混淆器，那么它们将可以应用在很多的密码学应用上，例如软件保护、构造全同态加密、去掉随机预言以及将对称加密方案转化成非对称加密方案。不幸地，Barak[2]证明了要构造一个安全的具有通用性的混淆器是不可能的。然而这个不可能的结论并没有排除存在只针对某种功能的混淆器，例如点函数[3－7]，重加密功能[8]，和签名后加密功能[1]。

我们构造了一个混淆器来实现对加密的环签名功能的混淆。加密的环签名功能（ERS）：签名者选择一个环 R，用自己的私钥和 R 对消息 M 进行环签名，然后用接收者的公钥对这个环签名进行加密。假设 Bob 是某个团体的成员，Bob 希望披露一些关于这个团体的信息给记者。最好的实现方法是 Bob 通过浏览器发送匿名的 email 给记者。这封 email 包含了 Bob 想披露的信息 M 以及对 M 的一个

* **收稿日期**：2013－03－22
基金项目：国家重点基础研究发展计划“973”资助项目（2011CB80800）
作者简介：陈兴发（1985 年生），男；**研究方向**：计算机与通信；E-mail：7131117532@163.com

环签名。这个环签名的环 R 应该包含 Bob 所在的团体的所有人的名字（当然也包含 Bob）。当然了，这封 email 所包含的所有信息都应该用记者的公钥进行加密。如果 Bob 的浏览器不能实现加密的环签名功能，Bob 可以将经过混淆以后具有加密的环签名功能的程序给邮件服务提供商，然后邮件服务提供商通过运行混淆以后的程序帮 Bob 生成加密过的环签名。我们预期如果环签名本身在标准模型下是匿名的和不可伪造的，那么这个环签名方案在敌手得到了相关的混淆程序以后还是匿名的和不可伪造的。但是当敌手得到了加密的环签名功能的混淆程序后，我们无法阻止敌手生成一个加密过的环签名。而且如果敌手还拥有接收者的私钥，那么这个环签名就不再是匿名的和不可伪造的。

Hada[1] 构造了特殊的签名后加密方案，使得先对消息进行签名再对签名进行加密的结果等价于先对签名的密钥进行加密再用加密过的签名密钥对消息进行签名的结果，所以 Hada 的实现签名后加密功能的混淆程序就只包含一个加密过的签名密钥和加密的公钥，即使敌手得到混淆程序，签名方案依然是存在不可伪造的。

Hada 的混淆器的构造是基于“对签名的加密等价于用加密后的密钥进行签名"。但对于加密的环签名来讲这个思路是不足够的。加密的环签名功能除了包含签名者的密钥以外还包含一个环 R，R 包含了签名者的公钥和其他人的公钥。在生成环签名过程中，签名者的公钥和其他人的公钥在处理上是不同的，很容易区分出来。如果混淆器仅仅对签名者的密钥进行加密，签名者的公钥和其他人的公钥在处理上依然是不同的，那么敌手在得到混淆程序以后就很容易知道真正的签名者是谁，这个环签名就不再是匿名的。

我们构造的混淆程序沿用 Hada 的思路并且将签名者的公钥和其他人的公钥在其密文的形式下进行处理，使得在敌手的角度来看所有人的公钥在处理上是一致的。这样当敌手得到混淆程序以后，环签名依然是匿名的和不可伪造的。

我们给出了当敌手得到具有加密的环签名混淆程序以后的环签名安全性定义。用 Waters 的环签名方案[9] 和线性加密方案[10] 构造出一个特殊的加密的环签名功能。而且还构造了一个安全的混淆器来实现对这个特殊的加密的环签名功能的混淆。在标准模型下，我们证明了构造的混淆器满足有关联预言的平均情况虚拟黑盒性质（ACVBP w. r. t. dependent oracles），Waters 的环签名方案在敌手获得混淆后的具有加密的环签名功能程序时依然是匿名的和不可伪造的。

本文是按以下顺序组织的：在第二部分我们给出了复杂性假设以及介绍了混淆器、公钥加密方案以及环签名的一些概念。在第三部分给出了当敌手得到具有加密的环签名混淆程序以后的环签名安全性定义。在第四部分我们介绍了关于混淆器的安全性定义，然后证明只要混淆器满足该安全性定义并且环签名本身在标准模型下是匿名的和不可伪造的，那么这个环签名方案在敌手得到了相关的混淆程序以后还是匿名的和不可伪造的。在第五部分我们描述了关于加密的环签名（ERS）功能的混淆器的具体构造，并证明它是满足在第四部分的混淆器的安全性定义。

1　预备知识

当 A 是一个概率算法时，$A(x_1, x_2, \cdots, x_k)$ 表示当 A 的输入是 $x_1, x_2, \cdots, x_k$ 时 A 的输出分布。当 S 是有限集合时，$x \leftarrow S$ 表示从集合 S 随机地取出一个元素。当 S 是一个概率分布时，$x \leftarrow S$ 表示根据 S 的分布取出一个元素。$\Pr[x_1 \leftarrow S_1; x_2 \leftarrow S_2; \cdots; x_k \leftarrow S_k: E]$ 表示当 $x_1 \leftarrow S_1$、$x_2 \leftarrow S_2$、$\cdots$、$x_k \leftarrow S_k$ 发生后，事件 E 发生的概率。如果函数 $\varepsilon(n): N \rightarrow \mathbf{R}^+$，对任意的多项式 $p(\cdot)$ 和所有充分大的 n 均有 $\varepsilon(n) < 1/p(n)$，那么函数 $\varepsilon(n)$ 称为可忽略的。

1.1　复杂性假设

G 是一个乘法循环群，它的阶 $n_0 = pq$. G_p 是 G 的 p 阶循环子群，G_q 是 G 的 q 阶循环子群。g 是 G 的生成元，h 是 G_q 的生成元。G_T 是乘法循环群，它的阶为 n_0。$e: G \times G \rightarrow G_T$ 是多项式时间内可计算的映射，并有如下性质：

①双线性：对所有的 $u, v \in G$ 和 $a, b \in Z$，有 $e(u^a, v^b) = e(u, v)^{ab}$

②非退化性：当 $< g > = G$ 时，均有 $< e(g, g) > = G_T$

假设 1（DL Assumption）对所有的多项式时间算法 D，

$$\left| \Pr\left[\begin{array}{l} a \leftarrow Z_q; b \leftarrow Z_q; r \leftarrow Z_q; s \leftarrow Z_q \\ d = D(q, h, (h^a, h^b), (h^{r+s}, (h^a)^r), (h^b)^s) \end{array} : d = 1 \right] - \Pr\left[\begin{array}{l} a \leftarrow Z_q; b \leftarrow Z_q; r \leftarrow Z_q; s \leftarrow Z_q; t \leftarrow Z_q \\ d = D(q, h, (h^a, h^b), (h^t, (h^a)^r), (h^b)^s) \end{array} : d = 1 \right] \right|$$

是可忽略的。

假设 2（CDH Assumption）对所有的多项式时间算法 A，

$\Pr[\eta \leftarrow G_p, a, b \leftarrow Z_p, c \leftarrow A(\eta, \eta^a, \eta^b, p): c = \eta^{ab}]$ 是可忽略的。

假设 3（Subgroup Hiding（SGH）Assumption）对所有的多项式时间算法 D，

$$|\Pr[w \leftarrow G: D(g, w, n_0) = 1] - \Pr[w \leftarrow G_q: D(g, w, n_0) = 1]|$$

是可忽略的。

1.2 混淆器的定义

一段程序可以看成是一个电路（circuit）。将 $\{C_n\}_{n \in N}$ 记为一类电路。其中 C_n 是一个多项式规模的电路的集合。C 的输入长度记为 $l_{in}(n)$，C 的输出长度记为 $l_{out}(n)$。

一个概率电路 $C(x)$ 可以看成是一个确定性的电路 $C(x, r)$，其中 x 是常规输入，r 是一个随机数。当常规输入 x 固定时，$C(x)$ 的输出的分布就是以 r 为随机数输入时运行 $C(x, r)$ 得到的分布。我们记两个电路输出的统计距离为 $\Delta(C_1(x), C_2(x)) = \sum_{y \in \{0,1\}^{l_{out}(n)}} |\Pr[o \leftarrow C_1(x): o = y] - \Pr[o \leftarrow C_2(x): o = y]|$

简单来讲，一个混淆器（obfuscator）是一个（多项式时间内，概率的）编译器，以一个电路 C 作为输入，然后输出一个让外人难以理解的电路 Obf (C)，而且 Obf (C) 实现的功能是和 C 一样的。

定义 1 设 Obf 是一个多项式时间算法，若对所有的 $n \in N$ 和所有 $C \in C_n$，有

$$\Pr[C' \leftarrow \text{Obf}(C): \forall x, \Delta(C(x), C'(x)) = 0] = 1$$

则称 Obf 是 $\{C_n\}_{n \in N}$ 的混淆器。

定义 1 只是说明了 Obf (C) 在功能上是和 C 一致，并没有说明安全性的要求。我们将在第四部分详细说明安全性的要求。

1.3 公钥加密体制和环签名的定义

我们来回顾公钥加密体制（PKE）的安全性 IND-CPA，选择明文攻击下的密文不可区分性质。我们的定义是基于［11］的。一个公钥加密体制包含三个算法（EKG, Enc, Dec）。EKG 是密钥生成算法，它以一个安全参数作 n 为输入，然手输出公钥和私钥（pk, sk）。Enc 是加密算法，以公钥 pk 和消息 m 作为输入，输出密文 c。Dec 是解密算法，以私钥 sk 和密文 c 作为输入，输出一个明文 m，假如 c 不是一个合法的密文则输出 $\perp$。

定义 2 （Indistinguishability of Encryptions against CPAs）设 Π =（EKG, Enc, Dec）是一个公钥加密体制。对于一个敌手 $A = (A_1, A_2)$，定义

$$Adv^{ind-cpa}_{PKE,A}(n) = \left| 2 \cdot \Pr\left[\begin{array}{c}(pk, sk) \leftarrow \text{EKG}(1^n);\\ (m_1, m_2, ht) \leftarrow A_1(pk);\\ b \leftarrow \{0,1\}; c \leftarrow \text{Enc}(pk, m_b);\\ b' \leftarrow A_2(pk, c, m_1, m_2, ht)\end{array}\right] - 1 \right|$$

如果对所有多项式时间的敌手 $A = (A_1, A_2)$，$Adv^{ind-cpa}_{PKE,A}(n)$ 都是可忽略的，那么 Π 满足 IND-CPA。

一个环签名方案包含三个算法：密钥生成算法（SKG），环签名算法（Sign）和验证算法（V）。密钥生成算法（SKG）输出公钥和私钥（pk, sk）。环签名算法（Sign）以（pk, sk）、消息 M 以及一个包含一族公钥的环 $R = \{pk_i\}_{i=1}^{l}$ 作为输入，输出一个环签名 σ。验证算法（V）以环 R、环签名 σ 和消息 M 作为输入，然后判断这个签名是不是有效的。

一个环签名方案应该满足匿名性（anonymity）和不可伪造性（unforgeability）。

定义 3 （Anonymity against Full Key Exposure）设 RS =（SKG, Sign, V）是一个环签名方案。对于一个敌手 $A = (A_1, A_2)$，定义

$$Adv^{anony-key}_{RS,A}(n) = \left| \Pr\left[\begin{array}{c}\{pk_i, sk_i\}_{i=1}^{l} \leftarrow \text{Setup}_{RS}(1^n);\\ R = \{pk_i\}_{i=1}^{l}; b \leftarrow \{0,1\};\\ (i_0, i_1, R', M, ht) \leftarrow A_1^{Sign}(R);\\ \sigma \leftarrow \text{Sign}(pk_{i_b}, sk_{i_b}, M, R');\\ b' = A_2^{Sign}(\sigma, R', M, \{sk_i\}_{i=1}^{l}, ht)\end{array}\right] - 1/2 \right|$$

如果对所有多项式时间的敌手 $A = (A_1, A_2)$，$Adv^{anony-key}_{RS,A}(n)$ 是可忽略的，那么 RS 是满足匿名性的。其中 Setup_{RS} 运行 l 次 SKG 得到了 l 对密钥。Sign 预言是以（s, R, M）（$pk_s \in R$）作为输入进行询问，然后以 σ = Sign（pk_s, sk_s, R, M）作为回复。

定义 4 （Existential Unforgeability against CMAs）设 RS =（SKG, Sign, V）是一个环签名方案。对于一个敌手 A，定义

$$Adv^{EU}_{RS,A}(n) = \Pr\left[\begin{array}{c}\{pk_i, sk_i\}_{i=1}^{l} \leftarrow \text{Setup}_{RS}(1^n);\\ \text{C\_ USER} \leftarrow \varnothing\\ (R^*, \sigma, m, Q) \leftarrow A^{Sign, Corrupt}(R);\\ \text{and } R^* \subseteq R \setminus \text{C\_ USER}\end{array}\right]$$

如果对所有多项式时间的敌手 A，$Adv^{EU}_{RS,A}(n)$ 是可忽略的，那么 RS 是存在不可伪造的。其中 Setup_{RS} 运行 l 次 SKG 得到了 l 对密钥。Sign 预言是以（s,

R, M）（$pk_s \in R$）作为输入进行询问，然后以 σ = Sign（pk_s, sk_s, R, M）作为回复。Corrupt 预言是以序号 s 作为输入进行询问。当敌手 A 询问 Corrupt（s）时，挑战者（challenger）就将 sk_s 告诉 A 并将 pk_s 添加到集合 C_USER 中。

2　有 ERS 混淆器的环签名的安全性定义

Π =（EKG, Enc, Dec）是一个公钥加密体制，RS =（SKG,Sign,V）是一个环签名方案。将两者结合起来，就形成我们要考虑的加密的环签名功能（ERS），记为 F_{ERS} = $\{F_n\}$（$n \in N$）。

ERS 的功能 $F_{pk,sk,R,pk_e} \in F_n$ 定义如下：

①当 F_{pk,sk,R,pk_e} 的输入是消息 m 时，它就先用 m、sk 和环 $R = \{pk_i\}_{i=1}^{l}(pk \in \mathbf{R})$ 生成一个环签名 σ，然后用 pk_e 将 σ 加密（$c \leftarrow E(pk_e, \sigma)$），然后输出 c。

②当 F_{pk,sk,R,pk_e} 的输入是一个特殊值 keys 时，它就输出（pk_e, R），其中 pk_e 是加密的公钥，R 是验证环签名的公钥集合。

我们定义一类电路 $C_{ERS} = \{C_n\}_{n \in N}$ 来实现 F_{ERS}，其中 C_{pk,sk,R,pk_e} 实现 F_{pk,sk,R,pk_e} 的功能。设 Obf 是 C_{ERS}的混淆器。下面我们考虑关于环签名的一种增强的安全性定义，就是考虑当敌手得到了混淆后的电路 Obf(C_{pk,sk,R,pk_e}) 时，环签名方案的匿名性和不可伪造性。

定义 5　（Anonymity w. r. t ERS Obfuscator）设 Π =（EKG, Enc, Dec）是一个公钥加密体制，RS =（SKG,Sign,V）是一个环签名方案，Obf 是 C_{ERS} 的混淆器。假如以下下条件成立，那么 RS 是在有 Obf 的情况下匿名的：对所有多项式时间的敌手 A = (A_1,A_2)，

$$\left|\Pr\left[\begin{array}{l}(pk_e,sk_e,\{pk_i,sk_i\}_{i=1}^{l}) \leftarrow \mathrm{Setup}_{ERS}(1^n); R = \{pk_i\}_{i=1}^{l} \\ i^* \leftarrow Z_l; C' \leftarrow \mathrm{Obf}(C_{pk_{i^*},sk_{i^*},pk_e,R}); b \leftarrow \{0,1\} \\ (i_0,i_1,R',M,ht) \leftarrow A_1^{Sign}(R,C') \\ \sigma \leftarrow \mathrm{Sign}(pk_{i_b},sk_{i_b},M,R') \\ b' = A_2^{Sign}(\sigma,R',M,\{sk_i\}_{i=1}^{l}C',ht)\end{array} : b = b'\right] - 1/2\right|$$

是可忽略的。

Setup_{ERS}运行 EKG 得到（pk_e, sk_e），然后运行 l 次 SKG 得到 l 对密钥。Sign 预言是以（s, R, M）（$pk_s \in R$）作为输入进行询问，然后以 σ = Sign（pk_s, sk_s, R, M）作为回复。

定义 6　（EU w. r. t. ERS Obfuscator）设 Π =（EKG, Enc, Dec）是一个公钥加密体制，RS =（SKG,Sign,V）是一个环签名方案，Obf 是 C_{ERS}的混淆器。假如以下下条件成立，那么 RS 是在有 Obf 的情况下存在不可伪造：对所有多项式时间的敌手 A，

$$\Pr\left[\begin{array}{l}(pk_e,sk_e,\{pk_i,sk_i\}_{i=1}^{l}) \leftarrow \mathrm{Setup}_{ERS}(1^n) \\ i \leftarrow Z_l; \mathrm{C\_USER} \leftarrow \emptyset \\ C' \leftarrow \mathrm{Obf}(C_{pk_i,sk_i,M,R}) \\ (R^*,\sigma,m,Q) \leftarrow A^{Sign,Corrupt}(R,C')\end{array} : \begin{array}{l}V(R^*,\sigma,m) = \mathrm{Accept\ and} m \notin Q \\ \mathrm{and}\ R^* \subseteq R \setminus \mathrm{C\_USER}\end{array}\right]$$

是可忽略的。

Setup_{ERS}运行 EKG 得到（pk_e, sk_e），然后运行 l 次 SKG 得到 l 对密钥。Sign 预言是以（s, R, M）（$pk_s \in R$）作为输入进行询问，然后以 σ = Sign（pk_s, sk_s, R, M）作为回复。当敌手 A 询问 Corrupt（s）时，挑战者（challenger）就将 sk_s 告诉 A 并将 pk_s 添加到集合 C_USER 中。

3　有关联预言的平均情况虚拟黑盒性质

平均情况虚拟黑盒性质（Average-case virtural black-box property 简称 ACVBP）是由 Hohenberger 在文［8］提出的。根据 ACVBP，Hohenberger 构造了一个安全的重加密功能的混淆器。但是 ACVBP 无法在加密的环签名功能上使用。在文［1］中，Hada 给出了有关联预言的平均情况虚拟黑盒性质（ACVBP w. r. t. dependent oracles）。在这个定义下，Hada 构造出一个安全关于加密的签名功能的混淆器。

定义 7　（ACVBP w. r. t. Dependent Oracles[1]）设 T（C）是一个与电路 C 相关的预言的集合。如果以下的条件成立，则称 C 的混淆器 Obf 满足有关联预言 T 的平均情况虚拟黑盒性质（ACVBP w. r. t. dependent oracle set T）：存在多项式时间算法 S，使得对所有的多项式算法 D（区分器），

$$\left|\Pr\left[\begin{array}{l}C \leftarrow C_n; \\ C' \leftarrow \mathrm{Obf}(C); \\ b \leftarrow D^{C,T(C)}(C')\end{array} : b = 1\right] - \Pr\left[\begin{array}{l}C \leftarrow C_n; \\ C'' \leftarrow S^C(1^n); \\ b \leftarrow D^{C,T(C)}(C'')\end{array} : b = 1\right]\right|$$

是可忽略的。

$D^{C,T(C)}$ 表示 D 可以以询问预言的方式询问 T（C）和 C。

下面的定理将说明环签名的安全性与有混淆器的环签名的安全性的关系。

定理 1　设 $T(C_{pk,sk,R,pk_e})$ 为 {Sign, Corrupt}。如果 C_{ERS} 的混淆器 Obf 满足有关联预言 $T(C_{pk,sk,R,pk_e})$ 的平均情况虚拟黑盒性质，那么环签

名的匿名性就意味着环签名在有 Obf 的情况下也是匿名的。

证明 证明过程运用 sequences games 的方法来证明。

Game 0 是有 ERS 混淆器的环签名匿名性的试验

Game 0：

$(pk_e, sk_e, \{pk_i, sk_i\}_{i=1}^{l}) \leftarrow \text{Setup}_{ERS}(1^n); R = \{pk_i\}_{i=1}^{l}; i^* \leftarrow Z_l;$

$C' \leftarrow \text{Obf}(C_{pk_{i^*}, sk_{i^*}, pk_e, R}); b \leftarrow \{0,1\};$

$(i_0, i_1, R', M, ht) \leftarrow A_1^{Sign}(R, C');$

$\sigma \leftarrow \text{Sign}(pk_{i_b}, sk_{i_b}, M, R');$

$b' = A_2^{Sign}(\sigma, R', M, \{sk_i\}_{i=1}^{l}, C', ht);$

记事件 S_0 为在 Game 0 里发生 $b = b'$。

下面我们构造算法 D，使得它的输出结果就是有 ERS 混淆器的环签名匿名性的试验的结果。

Game 1：

$(pk_e, sk_e, \{pk_i, sk_i\}_{i=1}^{l}) \leftarrow \text{Setup}_{ERS}(1^n); R = \{pk_i\}_{i=1}^{l}; i^* \leftarrow Z_l;$

$C' \leftarrow \text{Obf}(C_{pk_{i^*}, sk_{i^*}, pk_e, R});$

$b \leftarrow D^{C_{pk_{i^*}, sk_{i^*}, M, R}, Sign, Corrupt}(C')$

这里

$D^{C_{pk_{i^*}, sk_{i^*}, M, R}, Sign, Corrupt}(C')$

①$b \leftarrow \{0, 1\};$

②$(i_0, i_1, R', M, ht) \leftarrow A_1^{Sign}(R, C');$

③询问 $\text{Sign}(pk_{i_b}, sk_{i_b}, M, R')$ 后得到 σ；

④询问 Corrupt 得到 $\{sk_i\}_{i=1}^{l}$；

⑤ $b' \leftarrow A_2^{Sign}(\sigma, R', M, \{sk_i\}_{i=1}^{l}, C', ht);$

⑥If $b = b'$, output 1, else output 0。

记事件 S_1 为在 Game 1 中发生 $b = 1$。显然地 $\Pr[S_0] = \Pr[S_1]$。

下面我们用 S 来代替 Obf 的位置。

Game 2：

$(pk_e, sk_e, \{pk_i, sk_i\}_{i=1}^{l}) \leftarrow \text{Setup}_{ERS}(1^n); R = \{pk_i\}_{i=1}^{l}; i^* \leftarrow Z_l;$

$C' \leftarrow S^{C_{pk_{i^*}, sk_{i^*}, pk_e, R}};$

$b \leftarrow D^{C_{pk_{i^*}, sk_{i^*}, M, R}, Sign, Corrupt}(C')$ 。

记事件 S_2 为在 Game 2 中发生 $b = 1$。那么

$$|\Pr[S_1] - \Pr[S_2]| = \left| \Pr\begin{bmatrix} C \leftarrow C_n; \\ C' \leftarrow \text{Obf}(C); \\ b \leftarrow D^{C, T(C)}(C') \end{bmatrix}_{:b=1} - \Pr\begin{bmatrix} C \leftarrow C_n; \\ C'' \leftarrow S^C(1^n); \\ b \leftarrow D^{C, T(C)}(C'') \end{bmatrix}_{:b=1} \right|$$

由于 C_{ERS} 的混淆器满足满足有关联预言 $T(C_{pk,sk,R,pk_e})$ 的平均情况虚拟黑盒性质，所以 $|\Pr[S_1] - \Pr[S_2]|$ 是可忽略的。$\Pr[S_2]$ 应该为 $1/2 + \varepsilon$，ε 是可忽略的。如果 $\Pr[S_2] = 1/2 + \varepsilon_0$ 而且 ε_0 不是可忽略的，那么 A 和 S 可以构造一个新的敌手 $A_{RA} = (A_{RA,1}, A_{RA,2})$ 来攻破标准情况下的环签名的匿名性。

$A_{RA,1}^{Sign}(R)$

① $(pk_e, sk_e) \leftarrow \text{EKG}(1^n);$

② $C' \leftarrow S^C(1^n);$

③ $(i_0, i_1, R', M, ht) \leftarrow A_1^{Sign}(R, C');$

④ $ht' = (ht, C');$

⑤Output (i_0, i_1, R', M, ht') 。

当 S 要询问 C 时，$A_{RA,1}$ 询问 Sign 得到 σ 然后返回 $c = \text{Enc}(pk_e, \sigma)$ 给 S。

$A_{RA,2}^{Sign}(\sigma, R', M, \{sk_i\}_{i=1}^{l}, ht')$

① $ht' = (ht, C');$

② $b' \leftarrow A_2^{Sign}(\sigma, R', M, \{sk_i\}_{i=1}^{l}, C', ht);$

③Output b' 。

当 $\Pr[S_2] = 1/2 + \varepsilon_0$ 时，容易验证 $Adv_{RS, A_{RA}}^{anony-key}(n) = \varepsilon_0$。根据假设环签名是匿名的，因此 $A_{RA} = (A_{RA,1}, A_{RA,2})$ 是不可能攻破环签名的匿名性，所以 $\Pr[S_2] = 1/2 + \varepsilon$ 且 ε 是可忽略的。同时 $|\Pr[S_1] - \Pr[S_2]|$ 是可忽略的，故 $|\Pr[S_0] - 1/2|$ 是可忽略的，从而环签名方案在有 Obf 的情况下还是匿名的。

定理 2 设 $T(C_{pk,sk,R,pk_e})$ 为 {Sign, Corrupt}。如果 C_{ERS} 的混淆器 Obf 满足有关联预言 $T(C_{pk,sk,R,pk_e})$ 的平均情况虚拟黑盒性质，那么环签名的存在不可伪造性就意味着环签名在有 Obf 的情况下也是不可伪造的。

证明 证明过程运用 sequences games 的方法来证明。Game 0 是有 ERS 混淆器的环签名不可伪造性的试验。

Game 0：

$(pk_e, sk_e, \{pk_i, sk_i\}_{i=1}^{l}) \leftarrow \text{Setup}_{ERS}(1^n); i^* \leftarrow Z_l;$

$C' \leftarrow \text{Obf}(C_{pk_{i^*}, sk_{i^*}, pk_e, R});$

$(R^*, \sigma, m, Q) \leftarrow A^{Sign, Corrupt}(R, C');$

记事件 S_0 为在 Game 0 中发生 $V(R^*, \sigma, m) = \text{Accept and } m \notin Q \text{ and } R^* \subseteq R \setminus \text{C\_USER}$

下面我们构造一个算法 D，使得它的输出就是有 ERS 混淆器的环签名不可伪造性的试验的结果。

Game 1：

$(pk_e, sk_e, \{pk_i, sk_i\}_{i=1}^{l}) \leftarrow \mathrm{Setup}_{ERS}(1^n)$；$i \leftarrow Z_l$；

$C' \leftarrow \mathrm{Obf}(C_{pk_{i*}, sk_{i*}, pk_e, R})$；

$b \leftarrow D^{C_{pk_{i*}, sk_{i*}, M, R}, Sign, Corrupt}(C')$。

这里 $D^{C_{pk_{i*}, sk_{i*}, M, R}, Sign, Corrupt}(C')$

① $(R^*, \sigma, m, Q) \leftarrow A^{Sign, Corrupt}(R, C')$；

②If $V(R^*, \sigma, m) = \mathrm{Accept}$ and $m \notin Q$ and $R^* \subseteq R \setminus \mathrm{C\_USER}$, output 1, else output 0。

记事件 S_1 为在 Game 1 中发生 $b = 1$。显然 $\Pr[S_0] = \Pr[S_1]$。

下面我们用 S 来代替 Obf。

Game 2：

$(pk_e, sk_e, \{pk_i, sk_i\}_{i=1}^{l}) \leftarrow \mathrm{Setup}_{ERS}(1^n)$；$i \leftarrow Z_l$；

$C' \leftarrow S^{C_{pk_{i*}, sk_{i*}, M, R}}(1^n)$；

$b \leftarrow D^{C_{pk_{i*}, sk_{i*}, M, R}, Sign, Corrupt}(C')$。

记事件 S_2 为在 Game 2 中发生 $b = 1$。那么

$$|\Pr[S_1] - \Pr[S_2]| = \left| \Pr\begin{bmatrix} C \leftarrow C_n; \\ C' \leftarrow \mathrm{Obf}(C); \\ b \leftarrow D^{C, T(C)}(C') \end{bmatrix}_{:b=1} - \Pr\begin{bmatrix} C \leftarrow C_n; \\ C'' \leftarrow S^C(1^n); \\ b \leftarrow D^{C, T(C)}(C'') \end{bmatrix}_{:b=1} \right|$$

由于 C_{ERS} 的混淆器满足满足有关联预言 $T(C_{pk, sk, R, pk_e})$ 的平均情况虚拟黑盒性质，所以 $|\Pr[S_1] - \Pr[S_2]|$ 是可忽略的。

$\Pr[S_2]$ 应该是可忽略的，否则 A 和 S 可以构造出一个敌手 A_{EU} 来攻破标准情况的换签名的不可伪造性。

$A_{EU}^{Sign, Corrupt}(R)$：

① $(pk_e, sk_e) \leftarrow \mathrm{EKG}(1^n)$；

② $C' \leftarrow S^C(1^n)$；

③ $(R^*, \sigma, m, Q) \leftarrow A^{Sign, Corrupt}(R, C')$；

④Output (R^*, σ, m, Q)。

当 S 要询问 C 时，A_{EU} 通过询问 Sign 得到 σ，然后返回 $c = \mathrm{Enc}(pk_e, \sigma)$ 给 S。

容易验证 $Adv_{RS, A_{EU}}^{EU}(n) = Pr[S_2]$。根据假设 $Adv_{RS, A_{EU}}^{EU}(n)$ 是可忽略的，从而 $Pr[S_0]$ 也是可忽略的，故环签名在有 Obf 的情况下也是不可伪造的。

4　为特殊的 ERS 功能构造安全的混淆器

在这一部分，我们将为一个特殊的 ERS 功能构造一个混淆器，并且证明这个混淆器满足定义 7 的性质。这个特殊的 ERS 功能是由 Waters [9] 的环签名方案和线性加密方案[10]组合而成。

4.1　Waters 的环签名方案

全局初始化 可信的环签名初始化算法构造一个乘法群 G，其阶为 $n_0 = pq$。这个算法在选择 a，$b_0 \leftarrow Z_n$，然后计算 $A \leftarrow g^a$、$B_0 \leftarrow g^{b_0}{}_0$ 和 $\hat{A} \leftarrow h^a$。

设 $H: \{0,1\}^* \rightarrow \{0,1\}^{l_0}{}_0$ 是碰撞稳固的 hash 函数。初始化算法再选取 u'，u_1，u_2，…，$u_{l0} \leftarrow G$。

初始化算法输出 G 的描述、hash 函数 H、$(A, B_0, \hat{A})$ 以及 $(u', u_1, u_2, \cdots, u_{l0})$ 作为公共的参数。

SKG ()：

① $b \leftarrow Z_n$；

② $pk \leftarrow g^b$；

③ $sk \leftarrow A^b$；

④Output (pk, sk)。

Sign (pk, sk, R, M)：

① $(m_1, m_2 \cdots, m_{l_0}) \leftarrow H(M, R)$；$l = |R|$，$R = \{pk_i\}_{i=1}^{l}$；

②记 i^* 为使 $pk_{i^*} = pk$ 成立的序号；

③定义 $\{f_i\}_{i=1}^{l}$，$f_i = \begin{cases} 1, \text{if } i = i^* \\ 0, \text{otherwise} \end{cases}$；

④对每个 i，$1 \leqslant i \leqslant l$：$t_i \leftarrow Z_n$，$C_i \leftarrow (pk_i/B_0)^{f_i} h^{t_i}$，$\pi_i \leftarrow ((pk_i/B_0)^{2f_i - 1} h^{t_i})^{t_i}$，$t \leftarrow \sum_{i=1}^{l} t_i$；

⑤ $r \leftarrow Z_n$；$S_1 \leftarrow sk \cdot (u' \prod_{j=1}^{l_0} u_j^{m_j})^r \cdot \hat{A}^t$；$S_2 \leftarrow g^r$；

⑥Output $\sigma = ((S_1, S_2), \{C_i, \pi_i\}_{i=1}^{l})$。

V (R, M, σ)：

① $(m_1, m_2 \cdots, m_{l_0}) \leftarrow H(M, R)$；

② $\sigma = ((S_1, S_2), \{C_i, \pi_i\}_{i=1}^{l})$；

③对每个 i，$1 \leqslant i \leqslant l$，if $e(C_i, C_i/(v_i/B_0)) \neq e(h, \pi_i)$ then reject；

④ $C = \prod_{i=1}^{l} C_i$ if $e(A, B_0 C) = e(S_1, g) \cdot e(S_2^{-1}, u' \prod_{j=1}^{l_0} u_j^{m_j})^r)$ then accept, else reject。

定理 3[9]　如果假设 3 成立，那么 Waters 的环签名方案是匿名的。

定理 4[9]　如果 H 是碰撞稳固的且假设 2 成立，那么 Waters 的环签名方案是存在不可伪造的。

4.2　线性加密方案

EKG ()：

① $a \leftarrow Z_q$，$b \leftarrow Z_q$；

② $pk_e = (h^a, h^b)$，$sk_e = (a, b)$；

③Output (pk_e, sk_e)。

Enc (pk_e, m) $(m \in G)$:

①$r \leftarrow Z_q$, $s \leftarrow Z_q$;

② $c = (c_1, c_2, c_3) = ((h^a)^r, (h^b)^s, h^{r+s} \cdot m)$;

③Output c。

Dec (sk_e, c):

①$m = c_3 / (c_1^{1/a} \cdot c_2^{1/b})$;

②Output m。

定理 4[10] 如果假设 1 成立，那么线性加密方案就是 IND-CPA 的。

4.3 构造安全的加密环签名混淆器

我们特殊的 ERS 功能是由 Waters[9] 的环签名方案和线性加密方案[10]组合而成。特殊的 ERS 功能 $F_{pk,sk,R,pk_e} \in F_n$ 提供一下两个功能：

(i) $\mathrm{ERS}_{pk,sk,R,pk_e}(M)$:

① $((S_1, S_2), \{C_i, \pi_i\}_{i=1}^{l}) \leftarrow \mathrm{Sign}(pk, sk, R, M)$;

②$E(S_1) \leftarrow \mathrm{Enc}(pk_e, S_1)$;

③$E(S_1) \leftarrow \mathrm{Enc}(pk_e, S_2)$;

④对每个 i: $E(C_i) = \mathrm{Enc}(pk_e, C_i)$, $E(\pi_i) = \mathrm{Enc}(pk_e, \pi_i)$;

⑤ $\mathrm{Output}((E(S_1), E(S_1)), \{E(C_i), E(\pi_i)\}_{i=1}^{l})$。

(ii) $\mathrm{Keys}_{pk,sk,R,pk_e}(keys)$:

①Output (pk_e, R)。

我们定义了一族电路 $C_{ERS} = \{C_n\}_{n \in N}$来实现 ERS 功能，其中 $C_{pk,sk,R,pk_e} \in C_n$ 是实现 F_{pk,sk,R,pk_e} 的。我们为 C_{ERS}构造的混淆器 Obf 如下：

$\mathrm{Obf}(C_{pk,sk,R,pk_e})$:

①从 C_{pk,sk,R,pk_e} 中得到 pk, sk, R, pk_e;

② $k = (k_1, k_2, k_3) = E(pk_e, sk) = ((h^a)^r, (h^b)^s, h^{r+s} \cdot sk)$;

③$R = pk_i$, 令 i^* 为使 $pk^* = pk$ 成立的序号，定义 $\{f_i\}_{i=1}^{l} f_i = \begin{cases} 1, \text{if i} = i^* \\ 0, \text{otherwise} \end{cases}$;

④对于每个 i, $1 \leqslant i \leqslant l$, 计算

$d_i = (d_{i1}, d_{i2}, d_{i3}) = \mathrm{Enc}(pk_e, (pk_i / B_0)^{f_i})$, $e_i = (e_{i1}, e_{i2}, e_{i3}) = \mathrm{Enc}(pk_e, (pk_i / B_0)^{2f_i - 1})$;

⑤ $C_{k,\{d_i\}_{i=1}^{l},\{e_i\}_{i=1}^{l},pk_e,R}$。

混淆以后的电路 $C_{k,\{d_i\}_{i=1}^{l},\{e_i\}_{i=1}^{l},pk_e,R}$ 将按以下方式运行：

(i) 如果输入是 $M \in \{0,1\}^*$

$C_{k,\{d_i\}_{i=1}^{l},\{e_i\}_{i=1}^{l},pk_e,R}(M)$:

① $(m_1, m_2 \cdots, m_{l_0}) \leftarrow H(M, R)$;

②$l = |R|$, 对每个 i, $1 \leqslant i \leqslant l$, 计算

$t_i \leftarrow Z_n$, $E(C_i) = (d_{i_1}, d_{i_2}, d_{i_3} \cdot h^{t_i}), E(\pi_i) = (e_{i_1}^{t_i}, e_{i_2}^{t_i}, (e_{i_3} \cdot h^{t_i})^{t_i})$;

③ $r \leftarrow Z_n, E(S_1) = (k_1, k_2, k_3 \cdot (u' \prod_{j=1}^{l_0} u_j^{m_j})^r \cdot \hat{A}^t), E(S_2) = \mathrm{Enc}(pk_e, g^r)$;

④对每个 i, $1 \leqslant i \leqslant l$, 计算

$E'(C_i) = \mathrm{ReRandom}(pk_e, E(C_i)), E'(\pi_i) = \mathrm{ReRandom}(pk_e, E(\pi_i))$;

⑤ $E'(S_1) = \mathrm{ReRandom}(pk_e, E(S_1))$;

⑥Output $(E'(S_1), E(S_2), \{E'(C_i), E'(\pi_i)\}_{i=1}^{l})$。

(ii) 如果输入是一个特殊值 keys 那么 $C_{k,\{d_i\}_{i=1}^{l},\{e_i\}_{i=1}^{l},pk_e,R}$ 就输出 (pk_e, R)。

函数 ReRandom 按如下方式运行：

ReRandom (pk_e, c):

① $c = (c_1, c_2, c_3), pk_e = (h^a, h^b)$;

②r, $s \leftarrow Z_q$;

③ Output $((h^a)^r \cdot c_1, (h^b)^s \cdot c_2, h^{r+s} \cdot c_3)$。

定理 6 设 $T(C_{pk,sk,R,pk_e})$ 为 $\{\mathrm{Sign}, \mathrm{Corrupt}\}$，如果假设 1 成立，那么上面构造的 Obf 满足有关联预言 $T(C_{pk,sk,R,pk_e})$ 的平均情况虚拟黑盒性质。

证明 我们可以用 C_{ERS} 电路中的值 $(k, \{d_i\}_{i=1}^{3}, \{e_i\}_{i=1}^{3}, pk_e, R)$ 来代表一个电路。

构造多项式算法 S 如下：

$S^{C_{pk,sk,R,pk_e}}$:

①用 keys 作为输入询问预言 C_{pk,sk,R,pk_e} 来得到 pk_e, R;

② $sk' \leftarrow G$;

③ $k = (k_1, k_2, k_3) = \mathrm{Enc}(pk_e, sk')$

④对每个 i, $1 \leqslant i \leqslant l$, 计算

$d'_i \leftarrow G, e'_i \leftarrow G, d_i = \mathrm{Enc}(pk_e, d'_i), e_i = \mathrm{Enc}(pk_e, e'_i)$;

⑤Output $(k, \{d_i\}_{i=1}^{l}, \{e_i\}_{i=1}^{l}, pk_e, R)$。

下面我们将说明任何一个多项式时间的区分器即使在可以询问预言 $\mathrm{CRS} = \{C_{pk,sk,R,pk_e}, \mathrm{Sign}, \mathrm{Corrupt}\}$。的情况下都无法区分 S 输出的分布与真正的 Obf 输出的分布。

下面的证明运用 sequences games 的方法来证明。

我们定义 Game 0 为多项式时间区分器 D 的输入是一个真正的混淆以后的电路时的试验。

Game 0:

$\mathrm{GlobalSetup}(1^n)$;

$(pk_e, sk_e, \{pk_i, sk_i\}_{i=1}^{l}) \leftarrow \mathrm{Setup}_{ERS}(1^n)$;

$i^* \leftarrow Z_l, (pk, sk) = (pk_{i^*}, sk_{i^*}), R = \{pk_i\}_{i=1}^{l}$;

$(k, \{d_i\}_{i=1}^{l}, \{e_i\}_{i=1}^{l}, pk_e, R) \leftarrow \mathrm{Obf}(pk, sk, R, pk_e)$;

$b \leftarrow D^{CRS}(k, \{d_i\}_{i=1}^{l}, \{e_i\}_{i=1}^{l}, pk_e, R)$;

定义事件 S_0 为在 Game 0 中发生 $b = 1$。那么

$$\Pr[S_0] = \Pr\left[\begin{array}{c} C \leftarrow C_n \\ C' \leftarrow \mathrm{Obf}(C) \\ b \leftarrow D^{C,T(C)}(C') \end{array} : b = 1\right]$$

Game 1：将 Game 0 进行一个小改动，用 G 中的一个随机元素的加密来代替 D 的输入 k 即加密过的签名密钥 sk。

GlobalSetup (1^n)；

$(pk_e, sk_e, \{pk_i, sk_i\}_{i=1}^{l}) \leftarrow \mathrm{Setup}_{ERS}(1^n)$；

$i^* \leftarrow Z_l, (pk, sk) = (pk_{i^*}, sk_{i^*}), R = \{pk_i\}_{i=1}^{l}$；

$(k, \{d_i\}_{i=1}^{l}, \{e_i\}_{i=1}^{l}, pk_e, R) \leftarrow \mathrm{Obf}(pk, sk, R, pk_e)$；

随机选择 $junk\_k \leftarrow G$；

$k' = \mathrm{Enc}(pk_e, junk\_k)$；

$b \leftarrow D^{CRS}(k', \{d_i\}_{i=1}^{l}, \{e_i\}_{i=1}^{l}, pk_e, R)$；

定义 S_1 为在 Game 1 中发生 $b = 1$。我们断定：

$$|\Pr[S_0] - \Pr[S_1]| \leqslant \frac{1}{2} Adv_{PKE,A}^{ind-cpa}(n)$$

为了证明这个判断是正确的，我们构造了一个敌手 $A_0 = (A_{0,1}, A_{0,2})$ 来攻击线性加密的 IND-CPA 性质。$A_{0,1}$ 按下方式生成一对消息 (m_1, m_2) 和 ht：

$A_{0,1}(pk_e)$：

① GlobalSetup(1^n), $\{pk_i, sk_i\}_{i=1}^{l} \leftarrow \mathrm{Setup}_{RS}(1^n)$, $i^* \leftarrow Z_l, (pk, sk) = (pk_{i^*}, sk_{i^*}), R = \{pk_i\}_{i=1}^{l}$；

②随机选择 $junk\_k \leftarrow G$；

③令 $m_1 = sk$, $m_2 = junk\_k$, $ht = (pk, sk, R, pk_e)$；

④Output (m_1, m_2, ht)。

给定一个密文 c（m_1 或 m_2 的密文），$A_{0,2}$ 利用区分器 D 去区分是 c 是 m_1 的密文还是 m_2 的密文。

$A_{0,2}(c, m_1, m_2, h)$：

①$ht = (pk, sk, R, pk_e)$；

② $(k, \{d_i\}_{i=1}^{l}, \{e_i\}_{i=1}^{l}, pk_e, R) \leftarrow \mathrm{Obf}(pk, sk, R, pk_e)$；

③ $b \leftarrow D^{CRS}(c, \{d_i\}_{i=1}^{l}, \{e_i\}_{i=1}^{l}, pk_e, R)$；

④Output b。

当 c 是 m_1 的密文时，运行 A_0 是就和 Game 0 的试验一样。当 c 是 m_2 的密文时，运行 A_0 是就和 Game 1 的试验一样。故

$$|\Pr[S_0] - \Pr[S_1]| = |\Pr[c = \mathrm{Enc}(m_1) \mid A_{0,2} = 1] - \Pr[c = \mathrm{Enc}(m_2) \mid A_{0,2} = 1]| \leqslant \frac{1}{2} Adv_{PKE,A}^{ind-cpa}(n)$$

Game j $(2 \leqslant j \leqslant l + 1)$ 与 Game $j-1$ 的差别很小。将 D 的输入 d_i 换成是 G 的一个随机元素的加密 d'_i。

Game j：

GlobalSetup (1^n)；

$(pk_e, sk_e, \{pk_i, sk_i\}_{i=1}^{l}) \leftarrow \mathrm{Setup}_{ERS}(1^n)$；

$i^* \leftarrow Z_l, (pk, sk) = (pk_{i^*}, sk_{i^*}), R = \{pk_i\}_{i=1}^{l}$；

$(k, \{d_i\}_{i=1}^{l}, \{e_i\}_{i=1}^{l}, pk_e, R) \leftarrow \mathrm{Obf}(pk, sk, R, pk_e)$；

随机选择 $junk\_k \leftarrow G$；

$k' = \mathrm{Enc}(pk_e, junk\_k)$；

对每个 i, $1 \leqslant i \leqslant j-1$, 随机选择 $junk\_d_i \leftarrow G$, 并计算 $d'_i = \mathrm{Enc}(pk_e, junk\_d_i)$, $b \leftarrow D^{CRS}(k', \{\{d'_i\}_{i=1}^{j-1}, \{d_i\}_{i=j}^{l}\}, \{e_i\}_{i=1}^{l}, pk_e, R)$；

记事件 S_j 为在 Game j 中发生 $b = 1$。

在 Game $l + j + 1$ $(1 \leqslant j \leqslant l)$ 中，我们将 D 的输入 e_i 用 G 的一个随机元素的加密 e'_i 来代替。

Game $l+j+1$：

GlobalSetup (1^n)；

$(pk_e, sk_e, \{pk_i, sk_i\}_{i=1}^{l}) \leftarrow \mathrm{Setup}_{ERS}(1^n)$；

$i^* \leftarrow Z_l, (pk, sk) = (pk_{i^*}, sk_{i^*}), R = \{pk_i\}_{i=1}^{l}$；

$(k, \{d_i\}_{i=1}^{l}, \{e_i\}_{i=1}^{l}, pk_e, R) \leftarrow \mathrm{Obf}(pk, sk, R, pk_e)$；

随机选择 $junk\_k \leftarrow G$；

$k' = \mathrm{Enc}(pk_e, junk\_k)$；

对每个 i, $1 \leqslant i \leqslant l$, 随机选择 $junk\_d_i \leftarrow G$, 并计算 $d'_i = \mathrm{Enc}(pk_e, junk\_d_i)$.

对每个 i, $1 \leqslant i \leqslant j$, 随机选择 $junk\_e_i \leftarrow G$, 并计算 $e'_i = \mathrm{Enc}(pk_e, junk\_e_i)$.

$b \leftarrow D^{CRS}(k', \{d'_i\}_{i=1}^{l}, \{\{e'_i\}_{i=1}^{j}, \{e_i\}_{i=j+1}^{l}\}, pk_e, R)$；

记事件 S_{l+j+1} 为在 Game $l+j+1$ 发生 $b=1$。

我们断言：

$$|\Pr[S_j] - \Pr[S_{j-1}]| \leqslant \frac{1}{2} Adv_{PKE,A}^{ind-cpa}(n) \quad (2 \leqslant j \leqslant 2l+1)$$

这个断言的证明与前面的类似。我们构造了一个敌手 $A_j = (A_{j,1}, A_{j,2})$ 来攻击线性加密的 IND-CPA 性质。当 $1 \leqslant j \leqslant l$ 时

$A_{j,1}(pk_e)$：

① GlobalSetup(1^n), $\{pk_i, sk_i\}_{i=1}^{l} \leftarrow \mathrm{Setup}_{RS}(1^n)$, $i^* \leftarrow Z_l, (pk, sk) = (pk_{i^*}, sk_{i^*}), R = \{pk_i\}_{i=1}^{l}$；

②随机选择 $junk\_d_j \leftarrow G$；

③令 $m_1 = d_j$, $m_2 = junk\_d_j$, and $ht = (pk, sk, R, pk_e)$；

④Output (m_1, m_2, ht)。

$A_{j,2}(c, m_1, m_2, h)$：

①$ht = (pk, sk, R, pk_e)$。

②$(k, \{d_i\}_{i=1}^{l}, \{e_i\}_{i=1}^{l}, pk_e, R) \leftarrow \mathrm{Obf}(pk, sk, R, pk_e)$.

③随机选择 $junk\_k \leftarrow G$，计算 $k' = \mathrm{Enc}(pk_e, junk\_k)$。

④对每个 i，$1 \leqslant i \leqslant j-1$，

随机选择 $junk\_d_i \leftarrow G$，并计算 $d'_i = \mathrm{Enc}(pk_e, junk\_d_i)$。

⑤$b \leftarrow D^{CRS}(k', \{\{d'_i\}_{i=1}^{j-1}, c, \{d_i\}_{i=j+1}^{l}\}, \{e_i\}_{i=1}^{l}, pk_e, R)$。

⑥Output b。

当 $l+1 \leqslant j \leqslant 2l$ 时

$A_{j,1}(pk_e)$：

① $\mathrm{GlobalSetup}(1^n), \{pk_i, sk_i\}_{i=1}^{l} \leftarrow \mathrm{Setup}_{RS}(1^n)$，$i^* \leftarrow Z_l, (pk, sk) = (pk_{i^*}, sk_{i^*}), R = \{pk_i\}_{i=1}^{l}$；

②随机选择 $junk\_e_{j-1} \leftarrow G$；

③令 $m_1 = e_{j-l}$，$m_2 = junk\_e_{j-l}$，$ht = (pk, sk, R, pk_e)$；

④Output (m_1, m_2, ht)。

$A_{j,2}(c, m_1, m_2, ht)$：

①$ht = (pk, sk, R, pk_e)$；

②$(k, \{d_i\}_{i=1}^{l}, \{e_i\}_{i=1}^{l}, pk_e, R) \leftarrow \mathrm{Obf}(pk, sk, R, pk_e)$；

③随机选择 $junk\_k \leftarrow G$，and $k' = \mathrm{Enc}(pk_e, junk\_k)$；

④对每个 i，$1 \leqslant i \leqslant l$，随机选择 $junk\_d_i \leftarrow G$，并计算 $d'_i = \mathrm{Enc}(pk_e, junk\_d_i)$；

⑤对每个 i，$1 \leqslant i \leqslant j-l-1$，随机选择 $junk\_e_i \leftarrow G$，并计算 $e'_i = \mathrm{Enc}(pk_e, junk\_e_i)$；

⑥$b \leftarrow D^{CRS}(k', \{d'_i\}_{i=1}^{l}, \{\{e'_i\}_{i=1}^{j-l-1}, c, \{e_i\}_{i=j-l+1}^{l}\}, pk_e, R)$；

⑦Output b。

所有 j 满足 $2 \leqslant j \leqslant 2l$，均有

$$|\Pr[S_j] - \Pr[S_{j-1}]| = |\Pr[c = \mathrm{Enc}(m_1) \mid A_{j,2} = 1] - \Pr[c = \mathrm{Enc}(m_2) \mid A_{j,2} = 1]| \leqslant \frac{1}{2} Adv_{PKE,A}^{ind-cpa}(n)$$

下面，我们将 Obf 去掉。

Game $2l+2$：

$\mathrm{GlobalSetup}(1^n)$；

$(pk_e, sk_e, \{pk_i, sk_i\}_{i=1}^{l}) \leftarrow \mathrm{Setup}_{ERS}(1^n)$；

$i^* \leftarrow Z_l, (pk, sk) = (pk_{i^*}, sk_{i^*}), R = \{pk_i\}_{i=1}^{l}$；

随机选择 $junk\_k \leftarrow G$；$k' = \mathrm{Enc}(pk_e, junk\_k)$；对每个 i，$1 \leqslant i \leqslant l$，随机选择 $junk\_d_i \leftarrow G$，并计算 $d'_i = \mathrm{Enc}(pk_e, junk\_d_i)$.

对每个 i，$1 \leqslant i \leqslant l$，随机选择 $junk\_e_i \leftarrow G$，并计算 $e'_i = \mathrm{Enc}(pk_e, junk\_e_i)$.

$b \leftarrow D^{CRS}(k', \{d'_i\}_{i=1}^{l}, \{\{e'_i\}_{i=1}^{l}, pk_e, R)$；

记事件 S_{2l+2} 为在 Game $2l+2$ 发生 $b = 1$。

在 Game $2l+1$ 中 Obf 的输出并没有影响到 D。容易验证

$$Pr[S_{2l+2}] = Pr[S_{2l+1}],$$

$$\Pr[S_{2l+2}] = \Pr\left[\begin{array}{c} C \leftarrow C_n \\ C' \leftarrow S^C(1^n) \\ b \leftarrow D^{C,T(C)}(C') \end{array} : b = 1\right]$$

最后将上面的综合起来，有

$$|\Pr[S_0] - \Pr[S_{2l+2}]| \leqslant (l + \frac{1}{2}) \cdot Adv_{PKE,A}^{ind-cpa}(n)$$

当假设 1 成立时，根据定理 5，$Adv_{PKE,A}^{ind-cpa}(n)$ 是可忽略的，所以我们构造的 Obf 满足有关联预言 $T(C_{pk,sk,R,pk_e})$ 的平均情况虚拟黑盒性质，从而 Waters 的环签名方案在有 ERS 混淆器的情况下还是匿名的和存在不可伪造的。由定理 1，3，和 6 可得推论 1。由定理 2，4，和 6 可得推论 2

推论 1 如果假设 1 和假设 3 成立，那么 waters 的环签名方案是有 ERS 混淆器的情况下匿名的。

推论 2 如果假设 1 和假设 2 成立，那么 waters 的环签名方案是有 ERS 混淆器的情况下存在不可伪造的。

5 结 论

我们为一个特殊的加密的环签名功能构造了一个安全的混淆器。在标准模型下，我们用 sequences games 的方法证明了构造的混淆器满足平均情况虚拟黑盒性质（ACVBP）。有了这个性质，即使敌手在获得混淆后的具有加密的环签名功能程序，环签名依然是匿名的和不可伪造的。

参考文献：

[1] HADA SATOSHI. Secure obfuscation for encrypted signatures[C]//EUROCRYPT 2010, LNCS, 2010, 6110: 92-112.

[2] BARAK BOAZ, GOLDREICH ODED, IMPAGLIAZZO RUSELL, et al. On the (im) possibility of obfuscating programs[C]// CRYPTO 2001, LNCS, 2001, 2139:1-18.

[3] CANETTI RAN, DAKDOUK RONNY RAMZI. Obfuscating point functions with multibit output[C]//EUROCRYPT 2008, LNCS, 2008, 4965: 489-508.

[4] Wee Hoeteck. On obfuscating point functions[C]//Pro-

ceedings of STOC 2005, 2005: 523 – 532.
[5] CANETTI RAN, VARIA MAYANK. Non-malleable obfuscation[C]// TCC 2009, LNCS, 2009, 5444: 73 – 90.
[6] LYNN BENJAMIN, PRABHAKARAN MANOJ, SAHAI AMIT. Positive results and techniques for Obfuscation [C]// EUROCRYPT 2004, LNCS, 2004, 3027: 20 – 39.
[7] GOLDWASSER S, KALAI YAEL TAUMAN. On the impossibility of obfuscation with auxiliary input[C]// FOCS 2005, 2005: 60.
[8] HOHENBERGER SUSAN, ROTHBLUM GUY N, SHELAT ABHI, et al. Securely obfuscating re-encryption [C]//TCC 2007, LNCS, 2007, 4392: 233 – 252.
[9] SHACHAM HOVAV, WATERS BRENT. Efficient ring signatures without random oracles [C]// PKC 2007, 2007, 4450: 166 – 180.
[10] BONEH DAN, BOYEN XAVIER, SHACHAM HOVAV. Short group signatures [C]. // CRYPTO 2004, LNCS, 2004, 3152: 227 – 242.
[11] BELLARE MIHIR, DESAI ANAND, POINTCHEVAL DAVID, et al. Relations amongnotions of security for public-key encryption schemes [C]//CRYPTO 98, LNCS, 1998, 1462: 26 – 45.

(上接第 7 页)

参考文献:

[1] 张雨浓, 杨逸文, 李巍. 神经网络权值直接确定法[M]. 广州: 中山大学出版社, 2010.
[2] 韩红桂, 甄博然, 乔俊飞. 动态结构优化神经网络及其在溶解氧控制中的应用[J]. 信息与控制, 2010, 39(3): 354 – 360.
[3] 常春, 陈怡群, 肖宏儒, 等. 基于神经网络图像分析的智能鲜茶叶分选机[J]. 中国农机化学报, 2013, 34(1): 137 – 141.
[4] 贾鹤鸣, 张利军, 齐雪, 等. 基于神经网络的水下机器人三维航迹跟踪控制[J]. 控制理论与应用, 2012, 29(7): 877 – 883.
[5] 习会峰, 汤立群, 何庭惠, 等. 基于神经网络和遗传算法的桥梁参数优化方法与分析[J]. 中山大学学报: 自然科学版, 2008, 47(增刊2): 46 – 49.
[6] 张月琴, 刘翔, 孙先洋. 一种改进的 BP 神经网络算法与应用[J]. 计算机技术与发展, 2012, 22(8): 163 – 166.
[7] 杨文光. 权值直接确定的三角型模糊前向神经网络[J]. 中山大学学报: 自然科学版, 2013, 52(2): 33 – 37.
[8] ZHANG Y N, CHEN J W, FU S B, et al. Weights and structure determination of multiple-input Hermit orthogonal polynomials neural network [C] // Control and Decision Conference (CCDC), IEEE, 2012: 1106 – 1111.
[9] 张雨浓, 李钧, 张智军, 等. SIMO 傅里叶三角基神经网络的权值直接确定法和结构自确定算法[J]. 信息与控制, 2011, 40(4): 507 – 513.
[10] 张雨浓, 劳稳超, 余晓填, 等. 两输入幂激励前向神经网络权值与结构确定[J]. 计算机工程与应用, 2012, 48(15): 102 – 106.
[11] 王进, 烤贾雨, 熊超, 等. 基于神经网络异或算法的误差演算[J]. 电子世界, 2012, (11): 87.
[12] YIN H, DONG H B, HU Y P. A new view on noise cleaning for classification[C] // Conference on Information Management and Engineering (ICIME), IEEE, 2011: 597 – 601.
[13] RAFAEL C G, RICHARD E W, STEVEN L E. 数字图像处理(MATLAB 版)[M]. 北京: 电子工业出版社, 2009:103 – 116.
[14] 邹阿金, 张雨浓. 基函数神经网络及应用[M]. 广州: 中山大学出版社, 2009:18 – 19.
[15] 张小勇, 徐香勤, 贾利新. 函数组线性无关性的研究[J]. 河南科学, 2013, 31(1):25 – 27.
[16] 盛骤, 谢式千, 潘承毅. 概率论与数理统计[M]. 第四版. 北京: 高等教育出版社, 2008:49.
[17] 张雨浓, 邓健豪, 金龙, 等. 唯一性逻辑及其 BP 神经网络侦测[J]. 中山大学学报: 自然科学版, 2013, 52(3):1 – 5.