一个标准模型下的匿名IBE方案

杨坤伟 李顺东
(陕西师范大学计算机科学学院 西安 710062)

摘 要 大多数基于身份的加密方案(Identity-based Encryption,IBE)不具备接收者匿名性。提出了一个匿名IBE方案,方案基于判定性双线性DH假设(Decisional Bilinear Diffie-Hellman,DBDH),对于选择明文攻击(Chosen Plaintext Attack,CPA)是安全的。最后,给出了方案正确性证明、匿名性分析以及安全性证明。方案的优势是加密过程不需要对运算、接收者匿名等。与Gentry的方案相比,本方案所基于的困难性问题更常见,弥补了DBDH假设下匿名IBE的空缺。

关键词 基于身份的加密,匿名,选择明文攻击,困难性假设
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.6.037

Anonymous Identity-based Encryption without Random Oracles

YANG Kun-wei LI Shun-dong
(School of Computer Science,Shaanxi Normal University,Xi'an 710062,China)

Abstract Most identity-based encryption(IBE) schemes do not have the recipient anonymity. This paper proposed a new anonymous IBE scheme based on the DBDH assumption. This scheme is secure against adaptive chosen plaintext attack. We analyzed the anonymity of the scheme and verified the correctness and security. Our scheme is superior in the recipient anonymity and it doesn't use pairing computations in the encryption. Compared to Gentry's scheme, our scheme is based on a more common difficulty assumption and makes up anonymous IBE vacancy under DBDH difficulty assumption.

Keywords Identity-based encryption, Anonymous, Chosen plaintext attack, Difficulty assumption

IBE的思想是Shamir[1]在1984年提出的。在IBE方案中,公钥设施(Public Key Infrastructure,PKI)无需分发公钥证书,用户的身份转化成长度为n的数学状态字符串后可以直接作为公钥,私钥生成中心(Private Key Generator,PKG)为每个用户生成各自的私钥。这就产生一个问题:发送者用接收者的身份信息作为公钥加密信息时,身份信息很容易被敌手获得。这在需要保护用户隐私的情况下是不允许的,例如匿名电子投票等。对于一个匿名IBE方案,敌手从密文中无法得到接收者的任何身份信息。所以研究匿名IBE是非常有必要的。

2001年,一个真正实用的IBE方案由美国密码学家Boneh和Franklin[2]提出,其利用椭圆曲线上的双线性Weil配对,并且在随机预言机模型下证明了其安全性。之后,许多IBE方案被提出[3],并且安全性证明都模仿Boneh-Franklin的归约证明过程。Boneh和Franklin的方案[2]是少有的自带匿名性的方案,不过他们在文中并没有明确提出这一点。然而Boneh-Franklin的IBE方案有一点不足:其安全性是在随机预言机模型下证明的。Canetti等人在文献[4]中指出在随机预言机模型下证明安全的方案实际上未必是安全的,因为在方案实际执行时,需要寻找具体的哈希函数来替换方案中的随机预言机。因此人们更青睐在标准模型下构造IBE方案。

匿名IBE的概念最先由Boneh等人[5]提出,他们论述了匿名IBE在可搜索的公钥加密中的用处,但是文中并没有给出一个具体的方案。2005年,Abdalla等人[6]提出了一个公开问题:在不依赖随机预言机模型下如何构造匿名IBE,并对之前Waters[7]和Boneh-Boyen[8]的IBE方案不能达到匿名性做出证明。

Waters的方案[7]中:给定两个身份ID_0,ID_1,设C是m由ID_b加密得到的密文,$b\in\{0,1\}$是待挑战的比特。敌手做以下计算:

(1)ID_1对应的身份向量结果:

$(u'\prod_{i\in V,ID_1}u_i)$

(2)$e(g,C_3);e(C_2,(u'\prod_{i\in V,ID_1}u_i))$。若两项相等,则可以确定是由$ID_1$加密,若不等则为$ID_0$加密。

Boneh-Boyen的IBE方案[8]中:假设存在一个敌手A,拥有公钥$params=(g,g_1,g_2,U,k)$,给定两个身份ID_0,ID_1,C是m由ID_b加密得到的密文,$b\in\{0,1\}$是待挑战的比特。敌手分别对$i\in\{1,\cdots,n\}$做以下计算:

$e(C_2,U_{i,ID_0[i]});e(P,C_{i+2})$

若对于所有的$i\in\{1,\cdots,n\}$,以上两项均相等,则输出ID_0,否则输出ID_1。

到稿日期:2014-06-10 返修日期:2014-09-18 本文受国家自然科学基金项目:云计算与云存储若干关键问题研究(61272435)资助。
杨坤伟(1990-),男,硕士生,主要研究方向为密码学与信息安全,E-mail:yangkunwei@163.com;李顺东(1963-),男,教授,博士生导师,主要研究方向为密码学与信息安全。

2011 年，Boneh 和 Boyen 在不依赖随机预言机模型下提出了两个新的选择身份安全的 IBE 方案[9]，方案具有高效性和实用性。

第一个匿名的 IBE 方案在 2005 年的一个密码会议中被提出，通过把身份信息随机分成两部分来保证不被识别。文中构造了一个抵抗选择身份攻击-选择明文攻击（sID-CPA）方案，方案构造过程中没有使用强困难假设。此后，Boyen 和 Waters 提出了一个真正意义上的匿名 IBE 方案[10]，但是该方案是基于身份的分层加密方案（HIBE）。针对当时很少有 IBE 方案能在不使用随机预言机模型的前提下同时具有适应性安全、公共参数很短、严谨归约等良好性质，2006 年，Gentry 在标准模型下提出了两个匿名 IBE 方案[11]，分别达到选择明文安全和选择密文安全。该方案具有很多良好的特性如公共参数很短、加密过程不需要进行任何双线性对计算，关键一点是方案基于判定性 q-ABDHE 困难性假设达到了严谨规约，即挑战者 B 成功的概率和时间复杂性完全等同于敌手 A。但是判定性 q-ABDHE 是一种相对少用的困难性假设，并且无法对比其困难性与 DBDH 问题的困难性的高低，再加上安全性还依赖于不确定的询问次数 q，所以很难说明 q-ABDHE 下的紧性规约比 DBDH 下的松散规约强。

本文受此启发，在标准模型下基于 DBDH 问题构造了一个匿名 IBE 方案。

1 预备知识

1.1 双线性映射

定义 1 设 G 是由 g 产生的循环加法群，它的阶是素数 p，G_1 是同阶的乘法循环群，映射 $e:G\times G\to G_1$ 有以下性质。

1）双线性：对于所有的 $u,v\in G,a,b\in Z_N$，可以得到 $e(u^a,v^b)=e(u,v)^{ab}$。

2）非退化性：映射不把 $G\times G$ 中的所有元素对映射到 G_1 中的单位元，即当 g 是 G 的生成元时，$e(g,g)$ 是 G_1 的一个生成元。

3）可计算性：对于任意的 $u,v\in G$，有一个有效的算法来计算 $e(u,v)$。

1.2 困难性假设

这一节将给出一些方案所需要的困难性假设[12]。

DH 问题（Diffie-Hellman problem）：给定一个大素数 q，一个大整数生成元 $g\in Z_q^*$，以及由大随机数 a,b 生成的 $g^a \bmod q$ 和 $g^b \bmod q$，要求找到 $g^{a\cdot b} \bmod q$。

DH 问题是 Diffie-Hellman 密钥交换算法安全性的基础，这种安全性是建立在有限域内计算离散对数的困难性的基础之上的。

BDH 问题（bilinear Diffie-Hellman problem）：设 G_1 和 G_2 为两个具有素数 q 阶的点群，$e:G_1\times G_1\to G_2$ 是一个双线性映射，P 是 G_1 的生成元，对于给定的 $\langle P,aP,bP,cP\rangle$，其中 $a,b,c\in Z_q^*$，计算 $W=e(P,P)^{abc}\in G_2$。

DBDH 问题（decisional bilinear Diffie-Hellman problem）：区分元组 $\langle g,g^a,g^b,g^c,e(g,g)^{abc}\rangle$ 和 $\langle g,g^a,g^b,g^c,e(g,g)^z\rangle$ 的分布，即判断 z 是否等于 $abc \bmod q$，其中 a,b,c 属于 q 阶的点群 Z_q^*。

q-BDHE 问题（decisional bilinear Diffie-Hellman exponent problem）：给定 $\langle h,g,g^x,g^{x^2},\cdots,g^{x^q},g^{x^{q+2}},\cdots,g^{x^{2q}}\rangle\in G_1^{2q+1}$，其中 $x\in Z_q^*$，计算 $e(g,h)^{x^{q+1}}\in G_2$。

q-ABDHE 问题（q-augmented bilinear Diffie-Hellman exponent problem）：给定 $\langle g',g'^{(xq+2)},g,g^x,g^{x^2},\cdots,g^{x^q},g^{x^{q+2}},\cdots,g^{x^{2q}}\rangle\in G_1^{2q+2}$，其中 $x\in Z_q^*$，计算 $e(g,g')^{x^{q+1}}\in G_2$。

2 基于身份的加密

2.1 基于身份加密的定义

一个基于身份的加密机制由 Setup、Extract、Encrypt 和 Decrypt 4 个随机算法组成。

Setup：输入安全参数 k，返回系统公开参数 *params* 和系统主密钥 *master-key*。系统公开参数包括：有限的消息空间 M 的描述和有限的密文空间 C 的描述。系统的公开参数 *params* 对外公布，秘密保存系统主密钥 *master-key*，仅为 PKG 所知。

Extract：输入 *params*、*master-key* 和一个任意的 $c=Encrypt(param,ID,m)$，返回对应的私钥 d。这里 ID 为一个作为公钥的任意长字符串，d 为其对应的私有的解密私钥。Extract 算法生成公钥的对应私钥。

Encrypt：输入 params，ID 和明文消息 $m\in M$，输出密文 $c\in C$。

Decrypt：输入 *params*，密文 $c\in C$ 和私钥 d，返回明文消息 $m\in M$。

这些算法必须满足一致性约束的标准，也就是说当 d 是由 Extract 算法生成的公钥 ID 对应的私钥时，有下述计算成立：对于任意的 $m\in M$，$Decrypt(params,c,d)=m$，这里 $c=Encrypt(param,ID,m)$。

2.2 安全模型

本节介绍选择密文攻击下匿名 IBE 方案的安全模型。安全性证明通过下述游戏进行，其中有两个参与者：A 为敌手，B 为挑战者。

Setup：B 执行 Setup 算法并把系统参数 params 发送给 A。

Phase1：A 适应性地进行下列询问：

Extract query〈ID〉：B 对身份 ID 执行 Extract 算法，并把对应的私钥返还给敌手。

Decrypt query〈ID,C〉：B 首先对身份 ID 执行 Extract 算法，然后用生成私钥解密密文 C，并把明文 M 或出错信息返还给 A。

Challenge：A 提交身份 ID_0，ID_1 和消息 M_0，M_1 给 B，其中 ID_0，ID_1 都没有在阶段 1 中执行过提取询问，B 随机选择 $j,k\in\{0,1\}$，计算 $C^*=Encrypt(params,ID_j,M_k)$ 并把 C^* 返还给 A。

Phase2：A 继续适应性地询问，但是不能对 ID_0，ID_1 进行提取询问，或者对 $\langle ID_0,C^*\rangle$ 和 $\langle ID_1,C^*\rangle$ 进行解密询问。

Guess：A 输出 $j',k'\in\{0,1\}$，如果 $j'=j,k'=k$ 则 A 赢得游戏。

称 A 为匿名的选择性密文安全（ANON-IND-ID-CCA2）敌手，其优势定义为 $Adv=|\Pr[j'=j\wedge k'=k]-\frac{1}{4}|$。

定义 2 一个具有 (t,q,ε)-ANON-IND-ID-CCA2 安全性的 IBE 系统为在 t 时间内所有 ANON-IND-ID-CCA2 挑战者至多产生 q 次询问，至多有 ε 的概率取得挑战成功。

在上述游戏中，敌手如果不能进行解密询问，则被称为 ANON-IND-ID-CPA 敌手。

定义 3 一个具有 (t,q,ε)-ANON-IND-ID-CPA 安全性的 IBE 系统为在 t 时间内所有 ANON-IND-ID-CPA 挑战者至

多产生 q 次询问，至多有 ε 的概率取得挑战成功。

3 具体方案

3.1 方案介绍

本节在标准模型下提出一个新的匿名 IBE 方案。设 G 和 G_T 是阶为 p 的循环群，映射 $e:G\times G\to G_T$ 是一个双线性映射。具体方案如下：

建立：系统参数生成如下：选取一个随机的生成元 $g\in G$，随机选取 $\alpha\in Z_p$，令 $g_1=g^\alpha$，再随机选取 $g_2,U(u_1,u_2,\cdots,u_n)\in G$。公共参数为 g,g_1,g_2,U，主密钥为 α。

对于 $i=1,\cdots,n$，定义函数 $F_i:Z_P\to G$，其中 $F_i(x)=g_1^x u_i$。

私钥生成：为身份 $ID=(v_1,\cdots,v_i)\in Z_p^i$ 生成对应的私钥，其中 $i\leqslant n$。PKG 生成一个随机数 $r\in Z_p$。输出私钥：

$$d=(d_1,d_2,d_3)=(g_2^\alpha\prod_{k=1}^{i}F_k(v_k)^r,g^r,\prod_{k=1}^{i}F_k(v_k)^{\frac{r}{\alpha}})$$

加密：使用身份 $ID\in Z_p$ 加密 $m\in G_T$，发送者选择随机的 $t,p\in Z_p$，并输出密文：

$$C=(C_1,C_2,C_3,C_4)$$

$$=(e(g_1,g_2)^t m,\prod_{k=1}^{i}F_k(v_k)^{(t+p)},g_1^p,g^t)$$

解密：如果 $C=(C_1,C_2,C_3,C_4)$ 是使用身份 ID 对 m 加密的有效密文，则接收者可以使用私钥 $d=(d_1,d_2,d_3)$ 解密。解密如下：

$$m=C_1\frac{e(d_2,C_2)}{e(d_1,C_4)e(d_3,C_3)}$$

3.2 正确性

如果 $C=(C_1,C_2,C_3,C_4)$ 是使用身份 ID 对 m 加密的有效密文，则可以作如下验证：

$$\frac{e(d_2,C_2)}{e(d_1,C_4)e(d_3,C_3)}$$

$$=\frac{e(g^r,\prod_{k=1}^{i}F_k(v_k)^{(t+p)})}{e(g_2^\alpha\prod_{k=1}^{i}F_k(v_k)^r,g^t)e(\prod_{k=1}^{i}F_k(v_k)^{\frac{r}{\alpha}},g_1^p)}$$

$$=\frac{e(g^r,\prod_{k=1}^{i}F_k(v_k)^t)e(g^r,\prod_{k=1}^{i}F_k(v_k)^p)}{e(g_1,g_2)^t e(\prod_{k=1}^{i}F_k(v_k)^r,g^t)e(\prod_{k=1}^{i}F_k(v_k)^{\frac{r}{\alpha}},g^{\alpha p})}$$

$$=\frac{1}{e(g_1,g_2)^t}$$

所以，$m=C_1\frac{e(d_2,C_2)}{e(d_1,C_4)e(d_3,C_3)}$。

3.3 匿名性

设敌手想要验证的身份为 ID^*，首先计算 $ID^*=(v_1^*,\cdots,v_i^*)$ 对应的函数 $\prod_{k=1}^{i}F_k(v_k^*)$。由密文的构造可以发现，敌手想验证加密所用的身份，只能通过验证 $e(\prod_{k=1}^{i}F_k(v_k^*)^{(t+p)},g)=e(\prod_{k=1}^{i}F_k(v_k^*)^t,g)e(\prod_{k=1}^{i}F_k(v_k^*)^p,g)$ 来实现。显然，$e(\prod_{k=1}^{i}F_k(v_k^*)^t,g)$ 通过 $e(\prod_{k=1}^{i}F_k(v_k^*),C_4)$ 容易算出。但是，敌手不知道主密钥 α，所以无法通过 C_3 得到 p，从而无法算出 $e(\prod_{k=1}^{i}F_k(v_k^*)^p,g)$。由此可见，方案具备对接收者匿名的特性。

3.4 效率分析

加密过程：$e(g_1,g_2)$ 可以进行预运算，所以加密不需要进行双线性对运算。另外，加密过程中进行了 4 次幂运算和 1 次乘法运算，本方案与 Gentry 方案[11]相比有一定优势。

解密过程：需要 3 次双线性对运算，2 次乘法和 1 次除法运算。

下面给出本文方案与 Gentry 的方案[11]的详细对比，如表 1 所列。

表 1 方案对比

方案	私钥长度	密文长度	加密过程	解密过程
Gentry[11]	2	3	4r+2m+2i	1e+2m+1r
本文	3	4	4r+1m	3e+2m+1d

注：r 代表幂运算，m 代表乘法运算，i 代表逆运算，e 代表双线性对运算，d 代表除法运算

3.5 安全性

本节将基于判定性 BDH 困难问题证明上一节的 IBE 方案是 ANON-IND-ID-CPA 安全的。证明方法借鉴 Boneh 和 Boyen[13]的证明方法。

定理 1 假设 G 中的 DBDH 问题是困难的，则本文的 IBE 方案是 ANON-IND-ID-CPA 安全的。

证明：假设 A 拥有 ε' 的优势攻破上述 IBE 方案。可以构建一个算法 B，通过调用敌手 A 的能力来解决 G 中的 DBDH 问题。输入 g,g^a,g^b,g^c,T，如果 $T=e(g,g)^{abc}$ 则输出 1，否则输出 0。令 $g_1=g^a,g_2=g^b,g_3=g^c$，算法 B 的工作如下：

建立：B 生成系统参数，令 $g_1=g^a$，$g_2=g^b$，$g_3=g^c$。B 随机选取 $a_1,a_2,\cdots,a_n\in Z_p$，定义 $u_i=g_1^{a_i},i=1,\cdots,n$。B 将系统参数 $g,g_1,g_2,u_1,\cdots,u_n$ 发给敌手 A。定义函数 $F_i:Z_p\to G$。

$$F_i(x)=g_1^{x+a_i},i=1,\cdots,n$$

阶段 1：A 发起私钥提取询问，对于每一个 $ID=(v_1,\cdots,v_i)\in Z_p^i$，B 生成对应的私钥。B 选取一个随机数 $r\in Z_p$。生成私钥如下：

$$d=(d_1,d_2,d_3)$$

$$=(\prod_{k=1}^{i}F_k(v_k)^r,g^r g_2^{\frac{-1}{\sum(v_k+a_k)}},g^{r\sum(v_k+a_k)}g_2^{-1})$$

令 $r'=r-\frac{b}{\sum(v_k+a_k)}$，则

$$(1)\ d_1=\prod_{k=1}^{i}F_k(v_k)^r=g_2^\alpha g_1^{-b}\prod_{k=1}^{i}F_k(v_k)^r$$

$$=g_2^\alpha(g_1^{\sum(v_k+a_k)})^{\frac{-b}{\sum(v_k+a_k)}}g_1^{r\sum(v_k+a_k)}$$

$$=g_2^\alpha(g_1^{\sum(v_k+a_k)})^{r-\frac{b}{\sum(v_k+a_k)}}$$

$$=g_2^\alpha\prod_{k=1}^{i}F_k(v_k)^{r'}$$

$$(2)\ d_2=g^r g_2^{\frac{-1}{\sum(v_k+a_k)}}=g^{r-\frac{b}{\sum(v_k+a_k)}}=g^{r'}$$

$$(3)\ d_3=g^{r\sum(v_k+a_k)}g_2^{-1}=(g^{\sum(v_k+a_k)})^{r-\frac{b}{\sum(v_k+a_k)}}$$

$$=((g_1^{\sum(v_k+a_k)})^{\frac{1}{\alpha}})^{r-\frac{b}{\sum(v_k+a_k)}}$$

$$=\prod_{k=1}^{i}F_k(v_k)^{\frac{r'}{\alpha}}$$

所以，模拟的私钥：

$$d=(d_1,d_2,d_3)=(\prod_{k=1}^{i}F_k(v_k)^r,g^r g_2^{\frac{-1}{\sum(v_k+a_k)}},g^{r\sum(v_k+a_k)}g_2^{-1})$$

是对应身份 $ID=(v_1,\cdots,v_i)\in Z_p^i$ 的一个有效私钥。

挑战：敌手提交 2 个等长的消息 $M_0,M_1\in G_1$ 和 2 个消息 ID_0,ID_1。B 生成比特 $b,d\in\{0,1\}$，并按照阶段 1 的过程计算身份 ID_b 对应的私钥 d_{ID_b}。选取两个随机数 $c,\rho\in Z_p$ 构造 M_d 对应的密文：

$$C=(TM_d,\prod_{k=1}^{i}F_k(v_k)^{c+\rho},g_1^\rho,g^c)$$

假设 B 的分布是一个 BDH 元组，即 $T=e(g,g)^{abc}$，则密文形式为：

$$C=(e(g,g)^{abc}M_d,\prod_{k=1}^{i}F_k(v_k)^{c+\rho},g_1^{\rho},g^c)$$

$$=(e(g_1,g_2)^cM_d,\prod_{k=1}^{i}F_k(v_k)^{c+\rho},g_1^{\rho},g^c)$$

显然，C 是明文 M_d 的一个有效加密密文；否则，T 是 G 中的一个随机元素。这种情况下，从密文得不到 B 所选择的比特 d 的任何信息。

阶段 2：A 继续发起私钥提取询问，B 的回复同阶段 1。

猜测：最终，敌手 A 输出两个猜测 b'，$d'\in\{0,1\}$。如果 $b=b'$，$d=d'$，B 输出 1，否则输出 0。若分布 $T=(g,g)^{abc}$，则敌手 A 满足 $|\Pr[b'=b\wedge d'=d]-\frac{1}{4}|>\varepsilon$。若分布 $T\neq(g,g)^{abc}$，则 $\Pr[b'=b\wedge d'=d]=\frac{1}{4}$。因此有：

$$|\Pr[B(g,g^a,g^b,g^c,e(g,g)^{abc})=0]-\Pr[B(g,g^a,g^b,g^c,T=0)]|\geqslant|(\frac{1}{4}\pm\varepsilon)-\frac{1}{4}|=\varepsilon$$

以上是对定理 1 的证明。

4 方案对比

本节对上述方案和一些经典 IBE 方案进行对比。对比结果如表 2 所列。

表 2 方案对比

方案	复杂性假设	安全级别	匿名性
Waters[7]	BDH	CPA	no
Boneh-Boyen[13]	BDHI	sID-CPA	no
Gentry[11]	ABDHE	CPA	yes
本文	BDH	CPA	yes

结束语 自 2005 年 Abdalla 提出在不依赖随机预言机模型下如何构造匿名 IBE 这一公开问题以来，匿名 IBE 就成为密码学的一个研究热点。目前，匿名 IBE 方案并不是很多。本文受 Gentry[11] 启发，基于 DBDH 问题构建了一个标准模型下的匿名 IBE 方案，并对方案作了正确性证明、匿名性分析以及安全性证明。与文献[11]相比，本文方案在加密阶段更有优势。值得一提的是，本方案弥补了 DBDH 问题下匿名 IBE 的空缺且达到了 CPA 安全。在今后通信技术高速发展的时代，必然对 IBE 的设计提出更高的要求。如何在标准模型下构造安全性和效率都较高的 CCA 安全的方案是一个值得深入研究的问题。

参 考 文 献

[1] Shamir A. Identity-based Cryptosystems and Signature Schemes [C]// Wagner D, ed. Advances in Cryptology-Crypto'84, Lecture Notes in Computer Science. vol. 196, Berlin: Springer-Verlag, 1984: 47-53

[2] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[C]// Advances in Cryptology—CRYPTO 2001. Springer Berlin Heidelberg, 2001: 213-229

[3] Chatterjee S, Sarkar P. Identity-based encryption[M]. Springer, 2011

[4] Canetti R, Goldreich O, Halevi S. The random oracle methodology, revisited[J]. Journal of the ACM(JACM), 2004, 51(4): 557-594

[5] Boneh D, Di Crescenzo G, Ostrovsky R, et al. Public key encryption with keyword search[M]// Advances in Cryptology-Eurocrypt 2004. Springer Berlin Heidelberg, 2004: 506-522

[6] Abdalla M, Bellare M, Catalano D, et al. Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions[C]// Advances in Cryptology-CRYPTO 2005. Springer Berlin Heidelberg, 2005: 205-222

[7] Waters B. Efficient identity-based encryption without random oracles[M]// Advances in Cryptology-EUROCRYPT 2005. Springer Berlin Heidelberg, 2005: 114-127

[8] Boneh D, Boyen X. Secure identity based encryption without random oracles[M]// Advances in Cryptology-Crypto 2004. Springer Berlin Heidelberg, 2004: 443-459

[9] Boneh D, Boyen X. Efficient selective identity-based encryption without random oracles[J]. Journal of Cryptology, 2011, 24(4): 659-693

[10] Boyen X, Waters B. Anonymous hierarchical identity-based encryption(without random oracles)[M]// Advances in Cryptology-CRYPTO 2006. Springer Berlin Heidelberg, 2006: 290-307

[11] Gentry C. Practical identity-based encryption without random oracles[M]// Advances in Cryptology-EUROCRYPT 2006. Springer Berlin Heidelberg, 2006: 445-464

[12] 胡亮，刘哲理，孙涛，等. 基于身份密码学的安全性研究综述[J]. 计算机研究与发展，2009，46(9)：1537-1548
Hu Liang, Liu Zhe-li, Sun Tao, et al. Survey of Security on Identity-Based Cryptography[J]. Journal of Computer Research and Development, 2009, 46(9): 1537-1548

[13] Boneh D, Boyen X. Efficient selective-ID secure identity-based encryption without random oracles[M]// Advances in Cryptology-EUROCRYPT 2004. Springer Berlin Heidelberg, 2004: 223-238

(上接第 166 页)

[4] Petroni N L, Hicks M. Automated detection of persistent kernel control-flow attacks[C]// Proc. of the 14th ACM Conference on Computer and Communications Security. New York: ACM Press, 2007: 103-115

[5] Baliga A, Ganapathy V, Iftode L. Detecting kernel-level rootkits using data structure invariants[J]. IEEE Transactions on Dependable and Secure Computing, 2011, 8(5): 670-684

[6] Trusted Computer Group. TCG Specification Architecture Overview, version1. 2[EB/OL]. https://www.trustedcomputinggruop.org

[7] Intel® 6 4 and IA-3 2 Architectures Software Developer's Manual Volume 3B: System Programming Guide[R]. Intel Corporation, 1997-2009

[8] 李博，沃天宇，胡春明，等. 基于 VMM 的操作系统隐藏对象关联检测技术[J]. 软件学报，2013，24(2)：405-420
Li Bo, Wo Tian-yu, Hu Chun-ming, et al. Hidden OS Objects Correlated Detection Technology Based on VMM [J]. Journal of Software, 2013, 24(2): 405-420

[9] Hofmann O S, Dunn A M, Kim S, et al. Ensuring operating system kernel integrity with OSck[J]. ACM SIGPLAN Notices. ACM, 2011, 46(3): 279-290

[10] Gadaleta F, Nikiforakis N, Mühlberg J T, et al. Hyperforce: Hypervisor-enforced execution of security-critical code[M]// Information Security and Privacy Research, Springer Berlin Heidelberg, 2012: 126-137