基于身份的加密体制研究综述*

曾梦岐，卿 昱，谭平璋，杨 宇，周棟淞
（中国电子科技集团公司第三十研究所，成都 610041）

摘 要：着重对基于身份的加密（IBE）体制进行综述性的研究；通过与传统的 PKI 进行比较引出 IBE 加密体制，并介绍其通用的工作机制；接着对若干典型的基于身份的加密算法进行对比、分析，总结出各种算法的优劣；在 IBE 的已有实现和应用部分，跟踪了 IBE 的国际标准；最后对基于身份的加密体制中存在的热点问题进行剖析，提出有价值的问题供进一步研究。

关键词：基于身份的加密；PKI；椭圆曲线；双线性映射
中图分类号：TP309.2 **文献标志码**：A **文章编号**：1001-3695(2010)01-0027-05
doi:10.3969/j.issn.1001-3695.2010.01.007

Survey of research on identity-based encryption

ZENG Meng-qi, QING Yu, TAN Ping-zhang, YANG Yu, ZHOU Lian-song
(*The No. 30 Institute of China Electronic Technology Corporation, Chengdu* 610041, *China*)

Abstract: This paper focused on the general research on IBE scheme; demonstrated how IBE works by comparing traditional PKI and IBE, and then analyzed the pros and cons of some classic IBE algorithms by comparison. During the implementation and application of IBE, traced the international standard of IBE. Finally discussed some open problems, and proposed further some valuable questions.

Key words: identity-based encryption(IBE); PKI; ECC; bilinear maps

0 引言

IBE 也即基于标志的加密，是一种公钥密码体制，它直接利用用户的惟一身份标志作为公钥，不采用数字证书的概念，用户使用和后台管理都很简单，有广泛的应用前景。而在传统的 PKI 技术中，由于每个用户需要事先申请数字证书，用户使用复杂，后台管理也异常繁琐。为了让读者对 IBE 有个对比性的认识，表 1 给出了传统的 PKI 与 IBE 的比较。在 PKI 中 CA（certificate authority）对应 IBE 中的 TA（trusted authority），其中 PKG（private key generator）充当 TA 的角色。

表 1 传统的 PKI 与 IBE 的比较

功能	基于证书的 PKI	基于身份的 IBE
私钥生成	由用户或 CA 生成	由 PKG 生成
密钥证书	有	无
密钥分发	需要一个完整保护通道用于用户分发一个新的公钥到他的 CA	需要一个完整私有保护通道用于 TA 把新的私钥分发给他的持有者
公钥获取	从公共目录或密钥持有者获取	基于持有者的身份来动态获取
密钥托管	不需要（除非由 CA 生成私钥）	需要

下面介绍 IBE 的研究进展。

继 1976 年 Diffie 等人[1]提出了公钥密码学的概念之后，1984 年 Shamir[2]提出了基于身份的公钥密码体制（IBC）。IBC 主要包含两部分内容，即基于身份的加密（IBE）和基于身份的签名（IBS）。本文主要讨论 IBE。在 Shamir 提出的 IBE 体制中，存在着两个不容忽视的问题：a）如何向众多的可信第三方证明自己的身份；b）可信第三方如何安全地将用户的私钥送到用户手中。1987 年 Tanaka[3]基于离散对数问题和大整数的分解问题提出一个修改的 IBE 实现方案，并引入了门限的概念来解决该方案不抵抗合谋攻击的问题。1989 年 Tsuji 等人[4]使用 ELGamal 公钥密码系统，提出了一个基于离散对数问题的 IBE 方案。

第一个真正实用的 IBE 方案直到 2001 年才由 Boneh 等人[5]提出。该加密方案使用双线性对进行构造，基于双线性 Diffie-Hellman 假设，在随机预言机模型（random oracle model，ROM）下抵抗适应性选择密文攻击安全。此后，双线性映射函数成为构造基于身份密码系统的有力工具，大量的使用双线性映射函数构造的 IBE 方案被提出。但它有一个很大的缺点：计算效率较低，成为阻碍基于双线性对的密码系统走向实用的最大障碍。同年，Cocks[6]在不使用双线性映射函数的情况下，基于二次剩余假设提出了另一个 IBE 方案，但是依据带宽的要求，该方案非常低效，不实用。不使用双线性映射函数构造安全实用的 IBE 方案成为当时的一个开放性问题。在一般的 IBE 系统中，PKG 要产生私钥，安全传输私钥，负担过重，而且 PKG 知道私钥就可以解密任何用户的消息，即存在密钥托管问题。

为了降低 PKG 的负担，分层的 IBE 的概念首次由 Horwitz 等人[7]在 2002 年提出。同年，Gentry 等人[8]提出了一个安全实用的分层的 IBE 方案；Lynn[9]提出了一个提供不可否认性的可验证的 IBE 方案，该方案在 Boneh 等人[5]方案的基础上修

收稿日期：2009-04-21；修回日期：2009-06-26 基金项目：国家“863”计划资助项目（2008AA01Z405）

作者简介：曾梦岐（1981-），男，硕士，主要研究方向为存储安全、公钥密码学（zengmengqi518@163.com）；卿昱（1970-），女，高级工程师，硕士，主要研究方向为密码学、信息安全；谭平璋，男，硕士，主要研究方向为公钥密码学；杨宇，男，硕士，主要研究方向为公钥密码学；周棟淞，男，硕士，主要研究方向为公钥密码学。

改而成,效率较高。上述 IBE 方案的安全性分析一般都是在随机预言机模型 ROM 下进行的。2003 年,Canetti 等人[10]引入了安全性较弱的适应性选择身份选择密文攻击安全模型,并提出了一个 IBE 方案,在其方案安全性证明中无 random oracle。对于不使用 random oracle 的一些安全性分析,有时又称之为标准模型下的安全性分析。

同一作者在文献[11]中指出,使用任何选择明文攻击安全的 IBE 方案可以构造选择密文攻击安全的 IBE 方案,并给出了一个具体的 IBE 系统。但 Calletti 等人[10,11]把身份视为一个个字节的字符串,导致其系统对于身份中的每个字节要求一个双线性映射的计算,效率不高。Boneh 等人[12]提出了有效的 IBE 方案,在选择身份攻击安全模型下是安全的,并分别基于判定型双线性 Diffie-Hellman 假设和双线性 Diffie-Hellman 置换假设给出两个 IBE 系统。同一个作者在文献[13]中证明多项式时间安全的 IBE 方案可以在不使用 random oracle 的情况下存在,并给出一个具体的 IBE 方案,基于判定型双线性的 Diffie-Hallman 假设,但不幸的是由于其效率太低而不实用。

2005 年,Waters[14]提出了 Boneh 等人[13]方案的一个有效的改进版本,其安全性可以规约到判定型双线性 Diffie-Hellman 假设,但其缺点是公钥参数太长。与此同时,具有不同特征的 IBE 方案不断出现。一个带有关键字检索(key search)的 IBE 方案由 Boneh 等人[15]提出。Sahai 等人[16]提出了一个模糊的 IBE 方案,允许将生物特征作为公钥,用户的身份与用于加密的公钥身份之间可以有一定的误差。2005 年,Naccache 等人[17]对 Waters[14]的方案进行改进,提出了一个公钥参数较小的抵抗被动攻击安全的 IBE。同年 Boneh 等人[18]提出了一个分层的 IBE 系统,其密文仅由三个群元素组成,且不管层次的深度解密,只要求两个双线性映射的计算。该方案在选择身份攻击安全模型下安全,但安全性随层次深度指数级降低。2006 年,Abdalla 等人[19]介绍了一种带有通配符(wildcards)的 IBE 方案,允许加密消息到一定范围的身份满足一定类型的用户,这个类型通过一个固定的字符串序列和通配符来定义。在 2005 年的一次密码学会议上,匿名的 IBE 的概念被提出。2006 年,Boyen 等人[20]给出了匿名的 IBE 的具体实现,同时提出了匿名分层的 IBE 概念,并给出一个具体的实现方案。同年,Gentry[21]提出了第二个匿名的 IBE。该方案非常有效,但不幸的是方案依赖于一个较强的复杂性假设(扩展的双线性 Diffie-Hellman 指数假设),不能产生分层的 IBE。2007 年,Boneh 等人[22]在不使用双线性对的情况下,基于二次剩余假设,给出了一个空间有效的 IBE。

通过上述对 IBE 发展过程的分析可知,IBE 方案的设计主要有两个方向,其一是使用双线性映射函数来实现,这是自 2001 年 Boneh 等人提出第一个真正实用的 IBE 方案之后最突出的研究方向。但由于双线性映射函数构造的 IBE 存在计算效率较低的弱点,人们开始寻求一些其他方法,如使用二次剩余假设等,不使用双线性对来构造 IBE 方案,成为另一个重要的研究方向。同时,由于 IBE 方案本身所存在的密钥托管问题以及现实环境对 IBE 要求的不断增加,分层的 IBE 方案的设计和匿名的 IBE 方案的设计已经成为 IBE 方案设计基础上的重要的研究内容。

1 IBE 的工作机制

图 1 是一个通用的 IBE 工作模型。其中给出了 Alice 与 Bob 之间的安全通信的四个基本步骤:

a) Alice 用 Bob 的邮箱地址 bob@ b. com 作为公钥来加密自己的邮件。

b) 当 Bob 接收到消息后,他向密钥服务器(PKG)认证。而密钥服务器联系一个目录或其他的外部认证源来认证 Bob 的身份。

c) 认证完 Bob 以后,密钥服务器返回 Bob 的私钥。

d) Bob 用这个私钥来解密消息。

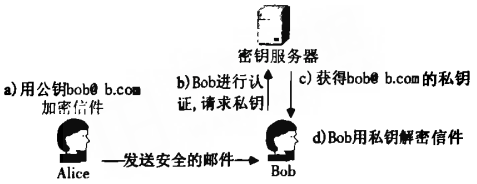

图1 基于身份的加密机制的工作过程

1984 年 Shamir 首先提出 IBE 的思想后,一些研究者包括 Shamir 本人,在 20 世纪 90 年代发布了一些基于身份的签名机制(IBS),或提出了各种 IBE 算法。尽管如此,大多数的算法均由以下四个随机算法组成:

a) 参数生成(setup)。选择安全参量 K 并获得 params(系统参量)和 master-key(主密钥)。系统参数包括有限消息空间 M 的描述和有限密文空间 C 的描述。显然,系统参数是公开的,而 master-key 只有 PKG 知道。这里 PKG 充当 TA 的角色。

b) 密钥生成(extract)。输入 params、master-key 和任意 $ID \in \{0,1\}^*$,获得私钥 d。其中 ID 是任意一条序列并作为公钥使用,d 是相对应的解密私钥。Extract 算法从给定的公钥析取私钥。

c) 加密(encrypt)。输入 params、ID 和 $M \in M$,获得密文 $C \in C$。

d) 解密(decrypt)。输入 params,$C \in C$ 和私钥 d,获得 $M \in M$。

这些算法必须满足一致性检测,即当 ID 给定,由 extract 析取出私钥 d 时,有 $M \in M$: decrypt(params, C, d) = M。其中,C = encrypt(params, ID, M)。

2 若干典型的 IBE 算法

2.1 Cocks IBE[5]

Cocks 的方案是基于数学难解问题——大整数分解的。

1)参数生成(setup) PKG 使用安全参数 t,生成两个质数 p、q,提供 $n = p \times q$,提供一个哈希函数 H(用来 hash 用户的 email-address)。(p、q)作为主钥,(n、H)作为系统参数。

2)密钥生成(extract) Bob 把自己的 ID 通过 hash 函数之后得到的 a 发送给 PKG,验证完身份之后,PKG 返回 r,满足 $r^2 = a \bmod n$。

3)加密和解密 使用对称方法,但是使用的是按位处理的方法,在传送方把密钥一位一位传送过去。在接收方恢复这个密钥,过程比较繁琐,使用网络带宽过大,占用运算所需内存也比较大。它每传递一个安全数据的一个位时,都要传递两个大整数。所以,当提供相同安全级别的加密方法时,如提供 1 024 bit的 RSA 模块时,就需要两个不同的 1 024 bit 数字,是带宽的要求变成 2 048。也就是说一个 80 bit 的对称密钥,要

求 20 KB 的数据传递(80 bit×2 048 = 163 840 bit = 20 KB),这使得应用这种加密方法处理日常商业交流变得难以实现,阻碍了它的发展[6]。

2.2 Boneh-Franklin(BF) IBE[5]

Boneh-Franklin 的方案是基于双线性映射,韦伊(Weil)配对原理。最终使用异或,保证明文异或两个实际上一样的值,那么就等于用明文异或"零",能够还原明文。

1)参数生成(setup)　PKG 使用安全参数 t 生成一个大质数 q,用 q 产生两个满足双线性映射的域 G_1、G_2。通俗一点讲就是一个椭圆曲线,在椭圆曲线上找一个点 P,随机生成数 s;s 作为主钥,s 与 P 的积 sP 作为系统参数;此外,PKG 也提供 hash 函数 H。

2)密钥生成(extract)　Bob 把 ID 发送给 PKG,通过身份验证后,PKG 生成私钥 $s\times H(\mathrm{ID})$(s 与 ID 的哈希值的积)发回给 Bob。

3)加密和解密　根据韦伊配对原理,$k=\mathrm{pair}(r\times \mathrm{ID}, s\times p)=\mathrm{pair}(s\times \mathrm{ID}, r\times p)$。可以证明这两个值相等,一个用来异或明文之后得到密文,在网络中传递;如果这两个都和明文异或,那么明文还是明文,也就是说只要用密文和剩下的那个数值 k 异或就能把密文还原为明文。

4)过程要求

Alice 可以知道的参数有:r(随机生成的),ID(Alice 知道的 Bob 的电子邮件地址,这是作为公钥的),$s\times p$(这是 PKG 系统生成的系统参数,发布给相关者的)。

Alice 传递给 Bob 的数据有:密文,$r\times p$。

Bob 可以知道的参数有:$s\times \mathrm{ID}$(PKG 计算出的私钥,返回给 Bob 的),$r\times p$(Alice 传递给 Bob 的)。

根据这些参数和数据,根据 3)的韦伊配对,可以看出 B-F 的 IBE 工作原理的正确性。

5)其他　利用阈值密码术,可以把存储在 PKG 主密钥分成多个块。主密钥的每个块可以存储在不同的地方,可用分布式存储,也不需要重新组合这些分散的块,不用在某个地方重新构造主密钥,合成分布的 PKG 就能够发布系统参数、主钥,然后生成使用者需要的私钥。根据 Bilinear-Diffie-Hellman 的假设,攻击者在随机预言机模型 ROM 是无法根据 PKG 发布的系统参数就能计算出私钥的。

2.3 Boneh-Boyen(BB1) IBE[12]

这个机制基于一个非标准的假设,叫做判定型 q-BDHI(decision Bilinear-Diffie-Hellman inversion)。G_1 表示一个阶数为 q 的双线性素数群。公钥 $\mathrm{ID}\in Z_q^*$,需要被加密的消息是 G_2 中的元素。

1)参数生成(setup)　PKG 选择一个生成元 $g\in_R G_1^*$,元素 $x, y\in_R Z_q^*$,并计算 $X=g^x$ 和 $Y=g^y$。

params:$\langle G_1, G_2, e, g, X, Y\rangle$ master-key:$\langle x, y\rangle$

2)KenGen　用来为公钥 $\mathrm{ID}\in Z_q^*$ 生成私钥:

a)选择随机数 $r\in_R Z_q$

b)计算 $K=g^{1/(\mathrm{ID}+x+ry)}\in G_1$

c)输出私钥 $d_{\mathrm{ID}}=(r, K)$

3)Encrypt　用来加密消息 $M\in G_2$(对应公钥 ID),选择随机数 $s\in_R Z_q^*$ 并输出密文如下:$C=(g^{r\cdot \mathrm{ID}}X^r, Y^r, e(g,g)s\cdot M)$;密文:$C=\langle U=g^{s\cdot \mathrm{ID}}X^r, V=Y^r, W=e(g,g)^s\cdot M\rangle\in G_1\times G_1\times G_2$。

4)Decrypt　用私钥 $d_{\mathrm{ID}}=(r, K)$ 来解密密文 $C=(U, V, W)$,输出明文 $M=W/e(UV^r, K)$。

2.4 Authenticated IBE[9]

除了需要一个额外的 hash 方法,本算法的 setup 和 extract 算法与 Boneh-Franklin IBE 一样。

1)参数生成(setup)　PKG 选择一个随机的生成元 $g\in G_1$,并选择一个密码 hash 函数 $H_1: F_q\times G_2\to\{0,1\}^n$,$H_2:\{0,1\}^*\to G_1$,$H_3:\{0,1\}^*\times\{0,1\}^*\to F_q$ 和 $H_4:\{0,1\}^n\to\{0,1\}^n$,对于特定的 n,还要选择一个主密钥 $s\in F_q$。

params:$\langle e, G_1, G_2, g, g^s, H_1, H_2, H_3, H_4\rangle$,master-key:$\langle s\rangle$

2)密钥生成(extract)　PKG 为身份为 IDA 的用户计算私钥 $d_A=H_2(\mathrm{ID}_A)^s$。

3)带认证的加密　用户 $A(\mathrm{ID}_A)$ 用另一个用户 $B(\mathrm{ID}_B)$ 的私钥 d_A 加密消息 $M\in\{0,1\}^*$ 如下:

a)选择随机数 $r\in_R\{0,1\}^n$。

b)计算 $c_1=H_3(r, M)$ 和 $c_2=e(d_A, H_2(\mathrm{ID}_B))$。

c)输出密文 $C=\langle r\oplus H_1(c_1, c_2), E_{H_4(r)}(M)\rangle$。

4)带认证的解密　用户 B 用 A 的 ID_A,他的私钥 d_B 和 params 解密密文$\langle U, V, W\rangle$,如下:

a)计算 $c_2=e(H_2(\mathrm{ID}_A), d_B)$;

b)$r=V\oplus H_1(U, c_2)$;

c)$M=D_{H_4(r)}(W)$;

d)比较 U 与 $H_3(r, M)$ 是否相等;

e)如果不相等,丢弃密文,否则输出明文 M。

2.5 Hierarchical IBE[8]

当 Boneh-Franklin 提出 IBE 实现方案时,他们仅仅考虑了一个 PKG 在两个使用者 Alice 和 Bob 进行消息传递的情况下。但是,当消息传递者增加之后,如果只有一个 PKG,则 PKG 负荷严重。后来有人提出的分层的 IBE 方案(HIBE),就是多个 PKG 具有一定的层次性,PKG 只为自己层次之下的实体计算私钥。HIBE 是结合了 IBE 技术的方案,但是又不像普通的 IBE 方案中,使用任意字符串作为公钥,HIBE 使用的是字符串元组作为公钥[18]。元组里的每个字符串代表了层次中的父节点。在技术改进过程中,由 2 层向 n 层发展。

2.6 若干典型的 IBE 算法的比较

这些可以应用的方法中,Cocks 提出的方法过于复杂,并且占用带宽过大,没有得到很大的发展,真正应用得不多;最常被提起并且被大量使用的技术是 Boneh-Franklin 提出的方法,使用了双线性映射,韦伊配对原理,比较经典;Ding-Tsudik 提出的方法利用了改进的 RSA 算法,其算法内容使用大数难分解原理,比较简单;Keyword Search 和 Hierarchical 思想都是 IBE 的进一步推广应用。表 2 给出了若干典型 IBE 算法的比较。

表 2　若干典型 IBE 算法的比较

IBE 算法	效率	安全性
Cocks	低效	容易受到适应性选择密文攻击
Boneh-Franklin	有效	Fullldent[5]可以抵抗选择明文攻击
Boneh-Boyen	有效	在无 random oracle 条件下可以证明是选择明文安全的
Authenticated	有效	随机预言机模型中可以抵抗适应性选择密文攻击
Hierarchical	高效	应用 Fujisaki-Okamoto 填充技术后可以抵抗选择密文攻击

3 IBE的实现和应用

由Boneh等人设计的IBE加密体制(Stanford IBE system)已经在Debian GNU/Linux下实现(源代码参考http://crypto.stanford.edu/ibe/download.html)。Shamus Software开发了一个密码库叫MIRACL,这个库里也包含了Boneh-Franklin的IBE密码体制。以上两者都是开源的。此外,Voltage Security也开发了自己的IBE库,并且已得到了工业上的应用。Voltage IBE主要运用Boneh-Franklin(BF)[5]和Boneh-Boyen(BB1)[12]。以上三者都是用C/C++开发的。同时爱尔兰National University的计算机安全与密码学研究组也提供开源的Java版本的IBE实现。表3给出了实现IBE的四个软件库。

表3 实现IBE的四个软件库

软件库	编程语言	是否开源	应用层次	IBE算法
Stanford IBE	C	是	学术研究	BF
MIRACL IBE	C++	是	学术研究	BF
Voltage IBE	C	否	工业企业	BF和BB1
National IBE	Java	是	学术研究	BF

此外,IBE的国际标准化进程也在进行中。2007年12月,IETF发布了RFC 5091[23]。其中给出了IBC标准——IBCS(identity-based cryptography standard)#1。这个标准描述了实现Bonel-Franklin IBE和Boneh-Boyen IBE算法的实现。2009年1月IETF发布了RFC 5408。其中给出了IBE的体系结构和数据结构支持[24]。RFC 5409给出了如何运用密码消息语法来使用Boneh-Franklin IBE和Boneh-Boyen IBE算法[25]。2008年4月,IEEE P1363.3草稿[26]发布,标准中定义了基于双线性映射(paring)的IBE草案。表4给出了IBE的国际标准化进程。

表4 IBE的国际标准化进程

组织	名称	时间	内容
IETF	RFC 5091	2007.12	基于身份的公钥密码标准(IBCS)#1
	RFC 5408	2009.1	IBE的体系结构和数据结构支持
	RFC 5409	2009.1	用密码消息语法来描述BF和BB1算法
IEEE	P1363.3	2008.4	基于双线性映射(paring)的IBE草案

IBE技术主要使用在电子邮件系统中。高度的信息化给企业和组织带来了巨大的生产力,越来越多的电子邮件交互提高了工作效率,所以电子邮件的安全性备受重视,电子邮件的安全应用受到各个企业和组织的关注。除了要求使用安全技术保证信息的隐私,保证内容的安全,还要求有很好的易用性和友好的界面等,最好是高效适用且易推广。

Proofpoint和Voltage是两个国外的应用实例:Proofpoint公司使用IBE技术构建了Secure Messaging;Voltage Security公司使用IBE技术构建了安全平台,并将IBE应用于工业中。

4 开放问题讨论

Boneh和Franklin利用双线性映射构造第一个安全实用的身份加密方案的创新性研究,使得基于身份的公钥密码系统重新成为了研究的热点。从BF-IBE提出以后,许多相关的改进引申的文章纷纷出现,提出了许多有效的基于身份的加密方案[9]、基于身份的签名方案[27]、基于身份的密钥协商方案等[28]及其他基于身份的密码方案[29]。但是在具体的基于身份的密码系统实施中还存在以下一些公开问题:

a)密钥托管。在基于身份的公钥密码中,用户的私钥是由KGC利用其系统范围的主密钥来生成的,KGC能够生成所有用户的私钥,因此密钥托管是基于身份的密码系统固有的性质。如果KGC有任何的不诚实行为或者主密钥的泄露,都将直接导致用户私钥的泄露,系统毫无保密性可言,这样攻击者就可以轻易地获取用户的信息和伪造用户的签名,包括用户已发生的借此私钥的秘密通信都将直接暴露。如何克服基于身份的公钥系统中密钥托管的局限,使得它适合在一些不允许密钥托管的应用使用是一个值得研究的方向。

b)密钥撤销。在基于身份的密码系统中,用户的公钥是由用户的身份信息获得,撤销用户的公钥相当于撤销用户的身份,而用户的身份信息大多是固定且不容易改变的,因此密钥撤销是ID-PKC面临的另一个难题。在基于证书的PKI体制中,CRL是一种最简单、最常用的证书撤销方法。由于CRL是定期发布的,不能保证证书撤销信息的实时性和准确性。而基于身份的公钥密码最大优点就是简化证书管理、非交互式通信带来的低通信成本和计算成本,因此,一种简单而有效的密钥撤销方法也是基于身份系统实用化过程中的重要组成部分。

c)安全模型。一个好的密码算法或协议首先应该是安全的,而安全问题的研究要归根到安全模型上,正确的安全模型能够很好地表现攻击者能力以及要达到的安全目标。目前比较好用的证明方法是随机预言机模型ROM。Boneh和Franklin在提出第一个实用的基于身份的加密方案的同时,扩展了传统公钥加密方案的适应性选择密文攻击(IND-CCA)安全模型,建立了IND-ID-CCA模型,允许攻击者询问非挑战实体的私钥,并证明了所提出的基于身份的加密方案在随机预言机模型下IND-ID-CCA是安全的。因此在研究新的基于身份密码系统时,应该准确而全面地分析攻击者的能力,根据需要达到的安全目标建立适应该密码系统的安全模型,作为证明该系统安全的基础。

5 结束语

IBE是公钥密码学中的研究热点。本文对PKI和IBE进行了优劣性对比,并简单介绍了IBE的工作过程。为了让读者对IBE算法有更深的了解,接着对集中典型的IBE算法进行了对比分析;还给出了IBE已有的实现和应用,并对基于身份的加密体制中存在的热点问题进行剖析,供IBE研究者参考。

参考文献:

[1] DIFFIE W, HELLMAN M E. New directions in cryptography[J]. IEEE Trans on Information Theory, 1976, IT-22(6):644-654.

[2] SHAMIR A. Identity-based cryptosystems and signature schemes [C]//Proc of Crypto'84. [S.l.]:Springer-Verlag, 1984:47-53.

[3] TANAKA H. A realization scheme for the identity-based cryptosystem [C]//Proc of Advances in Cryptology-Crypto'87. [S.l.]: Springer-Verlag, 1987:341-349.

[4] TSUJI S, ITOH T. An ID-based cryptosystem based on the discrete logarithm problem[J]. IEEE Journal on Selected Areas in Communication, 1989,7(4):467-473.

[5] 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. London, UK:Springer-Verlag, 2001:213-229.

[6] COCKS C. An identity based encryption scheme based on quadratic residues[C]//Proc of International Conference on Cryptography and

Coding. [S. l.]: Springer-Verlag, 2001:360-363.

[7] HORWITZ J, LYNN B. Toward hierarchical identity-based encryption [C]//Proc of Advances in Cryptology Eurocrypt' 02. [S. l.]: Springer-Verlag, 2002:466-481.

[8] GENTRY C, SILVERBERG A. Hierarchical ID-based cryptography [C]//Proc of Advances in Cryptology-Asiacrypt' 02. [S. l.]: Springer-Verlag, 2002:548-566.

[9] LYNN B. Authenticated ID-based encryption cryptology[R]. ePrint Archive Report 2002/072. 2002.

[10] CANETTI R, HALEVI S, KATZ J. A forward-secure public-key encryption scheme[C]//Proc of Advances in Crptology-Eurocrypt'03. [S. l.]:Springer-Verlag, 2003:255-271.

[11] CANETTI R, HALEVI S, KATZ J. Chosen-ciphertext security from identity based encryption[C]//Proc of Advances in Cryptology-Eurocrypt'04. [S. l.]: Springer-Verlag, 2004:207-222.

[12] BONEH D, BOYEN X. Efficient selective ID secure identity based encryption without random oracles[C]//Proc of Advances in Cryptology-Eurocrypt'04. [S. l.]: Springer-Verlag, 2004:223-238.

[13] BONEH D, BOYEN X. Secure identity based encryption without random oracles[C]//Proc of Advances in Cryptology-Crypto'04. [S. l.]: Springer-Verlag, 2004: 443-459.

[14] WATERS B R. Efficient identity-based encryption without random oracles [C]//Proc of Advances in Cryptology-Eurocrypt'05. [S. l.]: Springer, 2005:114-127.

[15] BONEH D, GRESCENZO G D, OSTROVSKY R, *et al*. Public key encryption with keyword search[C]//Proc of Advances in Cryptology-Eurocrypt'04. [S. l.]: Springer-Verlag, 2004:506-522.

[16] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]//Proc of Advances in Cryptology-Eurocrypt'05. [S. l.]: Springer, 2005: 457-473.

[17] NACCACHE D. Secure and practical identity-based encryption[J]. Information Security, 2007,1(2):59-64.

[18] BONEH D, BOYEN X, GOH E J. Hierarchical identity based encryption with constant size ciphertext[C]//Proc of Advances in Cryptology-Eurocrypt'05. Berlin: Springer-Verlag, 2005:440-456.

[19] ABDALLA M, CATALANO D, DENT A, *et al*. Identity-based encryption gone wild[C]//Proc of the 33rd International Colloquium Automata, Languages and Programming. [S. l.]: Springer-Verlag, 2006:300-311.

[20] BOYEN X, WATERS B. Anonymous hierarchical identity-based encryption(without random oracle)[C]//Proc of Advances in Cryptology. [S. l.]:Springer, 2006:290-307.

[21] GENTRY C. Practical identity-based encryption without random oracles[C]//Proc of Advances in Cryptology-Eurocrypt. [S. l.]:Springer-Verlag, 2006:183-189.

[22] BONEH D, GENTRY C, HAMBURG M. Space-efficient identity based encryption without pairings[EB/OL]. (2007). http://eprint. iacr. org/2007/177. pdf.

[23] BOYEN X, MARTIN L. Identity-based cryptography standard (IBCS) #1: supersingular curve implementations of the BF and BB1 cryptosystems [EB/OL]. (2007-12). http://www. ietf. org/rfc/rfc5091. txt.

[24] APPENZELLER G, MARTIN L. Identity-based encryption architecture and supporting data structures[EB/OL]. (2009-01). http://www. ietf. org/rfc/rfc5408. txt.

[25] MARTIN L, SCHERTLER M. Using the Boneh-Franklin and Boneh-Boyen identity-based encryption algorithms with the cryptographic message syntax(CMS)[EB/OL]. (2009-01). http://www. ietf. org/rfc/rfc5409. txt.

[26] WHYTE W, JOHNSON D B. Draft standard for identity-based public-key cryptography using pairings[EB/OL]. (2008-04). http://grouper. ieee. org/groups/1363/IBC/material/P1363. 3-D1-200805. pdf.

[27] BONEH D, BOYEN X. Short signatures without random oracles [C]//Proc of Advances in Cryptology-Eurocrypt' 04. [S. l.]: Springer-Verlag, 2004:56-73.

[28] CHEN L, KUDLA C. Identity based authenticated key agreement from pairings[R]. 2002.

[29] BAEK J, ZHENG Yu-liang. Identity-based threshold decryption[C]// Proc of Pracitce and Theory in Public Key Cryptography-PKC. [S. l.]: Springer-Verlag, 2004:262-276.

(上接第 26 页)

[17] CHENG C H, FU A W, ZHANG Yi. Entropy-based subspace clustering for mining numerical data[C]//Proc of the 5th ACM SIGKDD. San Diego, CA:[s. n.], 1999:84-93.

[18] NAGESH H, GOIL S, CHOUDHARY A. Adaptive grids for clustering massive data sets[C]//Proc of the 1st SIAM ICDM. Chicago, IL:[s. n.], 2001.

[19] 吴泉源, 刘江宁. 人工智能与专家系统[M]. 长沙:国防科技大学出版社,1995.

[20] KRIEGEL H P, KRÖGER P, ZIMEK A. Clustering high-dimensional data: a survey on subspace clustering, pattern-based clustering, and correlation clustering[J]. ACM Trans on Knowledge Discovery from Data, 2009,3(1):1-58.

[21] KRIEGEL H P, KRÖGER P, RENZ M. A generic framework for efficient subspace clustering of high-dimensional data[C]//Proc of International Conference on Data Mining. 2005.

[22] GAN Guo-jun, WU Jian-hong, YANG Zi-jiang. PARTCAT: a subspace clustering algorithm for high dimensional categorical data[C]// Proc of International Joint Conference on Neural Networks. 2006: 4406-4412.

[23] GOVAERT G. Simultaneous clustering of rows and columns[J]. Control and Cybernetics, 1995,24:437-458.

[24] MADEIRA S C, OLIVEIRA A L. Biclustering algorithms for biological data analysis: a survey[J]. IEEE/ACM Trans on Computational Biology and Bioinformatics, 2004,1(1):24-45.

[25] NADIF M, GOVAERT G. Block clustering with mixture model: comparison between different approaches[C]//Proc of International Symposium on Applied Stochastic Models and Data Analysis. Brest: [s. n.], 2005.

[26] BERKHIN P, BECHER J. Learning simple relations: theory and applications[C]//Proc of the 2nd SIAM ICDM. 2002:420-436.

[27] DHILLON I. Co-clustering documents and words using bipartite spectral graph partitioning[C]//Proc of the 7th ACM SIGKDD. San Francisco, CA:[s. n.], 2001:269-274.

[28] COSTA G, MANCO G, ORTALE R. A hierarchical model-based approach to co-clustering high-dimensional data[C]//Proc of ACM Symposium on Applied Computing. 2008: 886-890.

[29] TJHI W C, CHEN Li-hui. Robust fuzzy co-clustering algorithm[C]// Proc of the 6th International Conference on Information, Communications & Signal Processing. 2007:1-5.