本专著获得国家自然科学基金（编号：61103207）资助

杨浩淼　邱乐德◎著

基于身份的公钥密码体制的研究

Jiyu Shenfen De Gongyao Mima Tizhi De Yanjiu

电子科技大学出版社

本专著获得国家自然科学基金（编号：61103207）资助

杨浩淼　邱乐德◎著

基于身份的公钥密码体制的研究

Jiyu Shenfen De Gongyao Mima Tizhi De Yanjiu

电子科技大学出版社

图书在版编目（CIP）数据

基于身份的公钥密码体制的研究 / 杨浩淼，邱乐德著.
—成都：电子科技大学出版社，2012.4
ISBN 978-7-5647-1118-4

Ⅰ. ① 基… Ⅱ. ① 杨… ② 邱… Ⅲ. ① 公钥密码系统
Ⅳ. ① TN918.2

中国版本图书馆 CIP 数据核字（2012）第 031428 号

本专著获得国家自然科学基金（编号：61103207）资助

基于身份的公钥密码体制的研究

杨浩淼　邱乐德　著

出　　版：电子科技大学出版社（成都市一环路东一段 159 号电子信息产业大厦　邮编：610051）
策划编辑：闫　笛
责任编辑：汤云辉
主　　页：www.uestcp.com.cn
电子邮箱：uestcp@uestcp.com.cn
发　　行：新华书店经销
印　　刷：成都蜀通印务有限责任公司
成品尺寸：140mm×203mm　印张　8.5　字数　210 千字
版　　次：2012 年 4 月第一版
印　　次：2012 年 4 月第一次印刷
书　　号：ISBN 978-7-5647-1118-4
定　　价：25.00 元

前　言

在传统的公钥密码学中，公钥是与身份无关的随机字符串，公钥基础设施（PKI）通过签证中心颁发公钥证书来绑定公钥和身份。而在基于身份密码学（IBC）中，公钥是代表用户身份的任意字符串，可以直接从身份中提取，则证书和公钥目录是不必要的，因此简化了公钥的管理，并由此带来了不需要密钥信道的非交互式通信以及不需要证书校验，节约了计算和通信成本。尽管 IBC 简化了公钥和证书的管理，相比较传统的 PKI 有着天然的优势，但是具体的基于身份密码系统在实施中存在一些公开问题，例如缺乏有效的非交互式密钥吊销的完整解决方案，缺乏有效的可验证加密签名方案。这些问题不解决，基于身份密码系统在实践中的应用将受到很大限制。另一方面，双线性映射和基于标准模型的可证明安全是近几年密码学界的研究热点。本书围绕着基于身份密码系统存在的问题和研究热点在以下几个方面进行了研究，并取得了如下一些成果。

本书通过前向安全，简单而有效地解决了基于身份密码系统的密钥吊销的难题，分别构造了前向安全的基于身份的签名和加密方案，该签名和加密方案共享系统参数生成、密钥生成和密钥更新，组合起来，可以构建实践的非交互式密钥吊销的基于身份密码系统的完整解决方案。以此系统为基础，可以构建基于身份的 PKI 以替代传统的基于证书的 PKI。和传统 PKI 相比，基于身份的 PKI 在密钥的分发和管理方面具有内在的轻便性，可广泛应用于安全的 E-mail 系统、Ad-Hoc 网络系统等。

本书提出了构造可验证加密签名方案的通用方法，并基于

Gentry 短签名构造了一个有效的可验证加密签名方案，在标准模型下严格证明其安全性。和同类方案相比，该方案构造简单，有较短的公钥尺寸、较低的计算代价以及较紧的安全归约，是一个真正实践的无随机预言机的可验证加密签名方案，能够用于在线合同签署协议以保障公平交换。本书还基于 Paterson 等的基于身份签名方案，构造了第一个无随机预言机的基于身份的可验证加密签名方案。

本书首次对密钥信息部分的逐渐泄漏过程进行了研究，建立了密钥信息泄漏过程模型，并根据模型较为准确地估计密钥寿命，从而可以设置合适的密钥更新周期，而合适的密钥更新周期将在密钥安全性和更新代价之间取得平衡。本书的密钥泄漏建模和密钥寿命预估的方法可以应用到任何密码系统的秘密密钥。

本书给出了适合于非交互式密钥吊销的基于身份密码系统的两个应用：网格用户代理签名和手机短信息加密。前者提高了制造网格的效率和可扩展性，后者集成了嵌入式计算机、移动电子商务以及基于身份密码学技术。两者都体现了它的优良特性和重大实践价值，对基于身份密码系统的实用化具有示范意义。

作　者

2012 年 1 月

目　录

第1章 绪 论

本章介绍了基于身份密码学的研究背景和研究意义，分析了基于身份密码学的研究现状及有待解决的主要问题，并和传统公钥密码体制进行了比较。

1.1 基于身份密码学的研究背景和研究意义

信息安全是信息社会所关注的重要问题之一，而密码学是信息安全的核心技术。1949 年，信息论创始人 Shannon[1]发表了“Communication Theory of Secrecy Systems”，使对密码的研究从一门艺术变为一门科学，标志着密码学这门新学科的诞生；1976 年是密码学历史上重要的一年，为了满足军方及政府对信息安全的要求，美国确定了数据加密标准 DES，第一次公开了加密算法的细节，而把密码的安全性建立在对密钥的保密上。几乎同时，Diffie 和 Hellman[2]发表了“New Directions in Cryptography”，提出公钥密码的思想，标志着现代密码学的开端。

与传统密码体制相比，公钥密码体制的加密密钥与解密密钥不同，虽然加密解密速度较慢，但是较好地解决了传统密码体制中密钥分发和管理的难题，并能构造有效的数字签名方案，因此能够很好地为网络信息提供机密性、数据完整性、认证性和不可否认性等安全服务。

公钥密码体制是建立在单向陷门函数（One-way Trapdoor Function）上的，其安全性都是基于某种数学难题。1978 年，Rivest、Shamir 和 Adleman[3]提出了 RSA 公钥密码体制，其安全性基于大

整数因子分解的数学难题，RSA 是第一个实用的公钥密码体制，也是到目前为止应用最广泛的公钥密码体制。1985 年，ElGamal[4]提出了一种基于离散对数问题的公钥密码体制，称为 ElGamal 密码体制，后来的 Schnorr 签名体制[5]和数字签名标准 DSA[6]都是它的变形。1985 年，Koblitz[7]和 Miller[8]分别独立地提出了基于椭圆曲线离散对数问题的椭圆曲线密码体制，其短密钥高强度的特点使得它一直是密码学的研究热点之一。

在传统的公钥密码学中，公钥是与身份无关的随机字符串，存在如何认证公钥的真实性的问题。公钥基础设施（Public Key Infrastructure，PKI）通过使用可信任第三方——签证中心（Certification Authority，CA）颁发公钥证书的形式来绑定公钥和身份信息。不过，PKI 证书管理复杂，需要建造复杂的 CA，证书发布、吊销、验证和保存需要占用较多资源，这就限制了 PKI 在实时和低带宽的环境中的应用。

为了简化公钥证书的管理，在 1984 年，Shamir[9]革命性地引入了基于身份密码学（Identity-Based Cryptography，IBC）。在 IBC 中，公钥是代表用户身份的任意字符串，比如用户的名字、E-mail 地址、手机号码等；存在一个可信任的机构——私钥生成器（Private Key Generator，PKG），根据用户的身份生成相应的私钥：首先运行 Setup 算法，生成系统的全局参数（或者称为主公钥）和主密钥；然后运行 Extract 算法，输入主密钥和一个任意的身份 $ID \in \{0, 1\}^*$，输出相应的私钥。由于公钥直接从身份信息中提取，则证书和公钥目录是不必要的，因此简化了公钥的管理，并由此带来了不需要密钥信道的非交互式通信以及不需要证书校验，节约了计算和通信成本。

由于具有以上的优势，IBC 不仅受到广泛的关注与研究，而且开始取代传统的基于证书的公钥密码体制在很多领域得到应用，如安全 E-mail 系统、Ad-Hoc 网络等，因此对 IBC 关键技术

及其应用进一步的研究具有重要的理论和实践意义。

1.2 基于身份密码学的研究现状和有待解决的主要问题

1.2.1 研究现状

Shamir 在提出基于身份的公钥密码概念的同时，也给出了一个基于身份的签名（Identity-Based Signature，IBS）方案[9]，但直到 2001 年，Boneh 和 Franklin[10]才提出了第一个实用的基于身份的加密（Identity-Based Encryption，IBE）方案，该方案使用了双线性映射，并基于随机预言机模型（Random Oracles Model，ROM）证明了安全性。这之后，大量使用双线性映射构造的基于身份的密码方案[14][16][17][21][23][30]被提出，IBC 又成为近年来密码学界的一个研究热点。不过 ROM 是一个理想模型，基于 ROM 的安全并不一定意味着真实世界的安全，密码学家们又着手研究无随机预言机的，也就是基于标准模型的基于身份密码方案。下面分别从三个方面概述 IBC 的研究现状。

1．基于双线性映射的构造和基于标准模型的可证明安全

在 1993 年，Menzens、Okamoto 和 Vanstone 就利用双线性映射来攻击超奇异椭圆曲线上的离散对数问题，这就是著名的 MOV 攻击[11]。在 2000 年，Joux 利用双线性映射构造了一轮的三方 Diffie-Hellman 密钥协商协议[12]，这是双线性映射在密码学中首次正面的应用。在 2001 年，Boneh 和 Franklin 利用双线性映射构造了第一个实用的基于身份加密方案。这之后，出现了大量的基于双线性映射构造的密码方案，使用双线性映射来构造密码方案是近年来密码学界的一个研究热点。

双线性映射 e: $\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ 通常使用基于超奇异椭圆曲线的

Weil 对或 Tate 对来构造，Tate 对比 Weil 对具有更高的效率。如果 $\mathbb{G}_1 \neq \mathbb{G}_2$，使用 Barreto-Naehrig 曲线具有更短的点表示[13]。已经做了大量工作以提高对计算的效率[53][54][55]。

在 1993 年，为了分析某些密码学构造的安全性，Bellare 和 Rogaway 引入了随机预言机模型[68]，这是一个理想模型。简单地讲，随机预言机是一个公开可用的形如 H: $X \rightarrow Y$ 的函数，它均匀而随机的选自于所有形如 $h: X \rightarrow Y$ 的函数所构成的集合 $\{h: X \rightarrow Y\}$（假设 Y 是有限集），任何一方（包括攻击者）可以关于任意的 $x \in X$ 查询随机预言机，并收到响应 $H(x)$。随机预言机被用来建模诸如 SHA-1 之类的密码学 Hash 函数，对密码方案的可证明安全有巨大的推动作用，大量的密码方案的安全性都是基于随机预言机模型的取得。

注意到基于 ROM 的安全是对存在随机预言机的理想世界而言的，并不是一定意味着真实世界的安全。Canetti 等[15]以及 Bellare 等[69]的工作表明，一旦随机预言机用具体的 Hash 函数实例化，基于 ROM 的方案有可能是不安全的。它的意义更多在于指出设计密码方案值得注意的地方。设计无随机预言机的密码方案是近几年密码学界的又一个研究热点，在 2003—2007 年的美密会、欧密会和亚密会等密码学会议上，有不少这样的论文[14][16][17][18][29][106][133][134][135]。

2．基于身份加密

在 2001 年，Boneh 和 Franklin 为 IBE 所设计的安全模型[10]，扩展自传统公钥加密的安全模型：它允许攻击者发布私钥查询，而且质询（Challenge）身份 ID^* 是攻击者适应性选择的。他们基于 ROM 证明了所提出的 IBE 方案的安全性，而基于标准模型的 IBE 方案在当时仍然是一个困难性问题。

为构造基于标准模型的 IBE 方案，首先是 Canetti 等[14]为 IBE 设计了一个较弱的安全模型，称之为选择身份（selective-ID，sID）

模型：攻击者在生成系统参数之前选择质询身份 ID^*，也就是说，ID^*是非适应性选择的，他们也提出了一个 IBE 方案，并基于标准模型证明其是选择身份安全的。接着 Boneh 和 Boyen[16]改进了上述结果，提出了一个更有效的选择身份安全的 IBE 方案。然后 Boneh 和 Boyen 还提出了一个完全安全的，也就是说 ID^*是适应性选择的，无随机预言机的 IBE 方案[106]，不过效率太低而不能用于实践，只是表明基于标准模型的完全安全的 IBE 方案是存在的。最后 Waters 对[16]中方案做了一处小的改动，提出了第一个有效的基于标准模型的完全安全的 IBE 方案[17]。

作为对不使用随机预言机的补偿，上述 IBE 方案的主公钥都是相当大的。例如，在 Waters 方案中，如果使用 160-bit 的抗碰撞 Hash 函数，主公钥将包含大约 160 个群元素，10kB 的存储量，并不能很好地适用于实践。在 2006 年的欧密会上，Gentry 提出了一个实践的完全安全的无随机预言机的 IBE 方案[18]，其主公钥仅包含 3 个群元素。

IBE 作为基于身份密码学的基本用语，可扩展以构建层次化 IBE[50][108][130]，模糊 IBE[129]，前向安全 IBE[109]等。而且 Moni-Naor 观察到，抵抗适应性选择身份攻击的 IBE 方案能够转换成抵抗适应性选择消息攻击的公钥签名方案[10]，上述大多数 IBE 方案都相应存在高效而安全的公钥签名方案[117][118][119]。另外，选择身份安全的 IBE 方案和强不可伪造的公钥签名方案的组合[112][113]，能够得到标准模型下适应性选择密文安全的公钥加密方案，其性能足可以和 Gramer-Shoup 方案[111]相媲美。

3．基于身份签名

早在 1984 年，Shamir 就给出了第一个 IBS 方案[9]。这之后，Fiat-Shamir IBS[19]、Guillou-Quisquater IBS[20]等 IBS 方案相继被提出。跟随着 Boneh 和 Franklin 将双线性映射引入到 IBE，Paterson[21]将双线性映射引入到 IBS。在 2003 年，Cha 和 Cheon[22]定义了 IBS