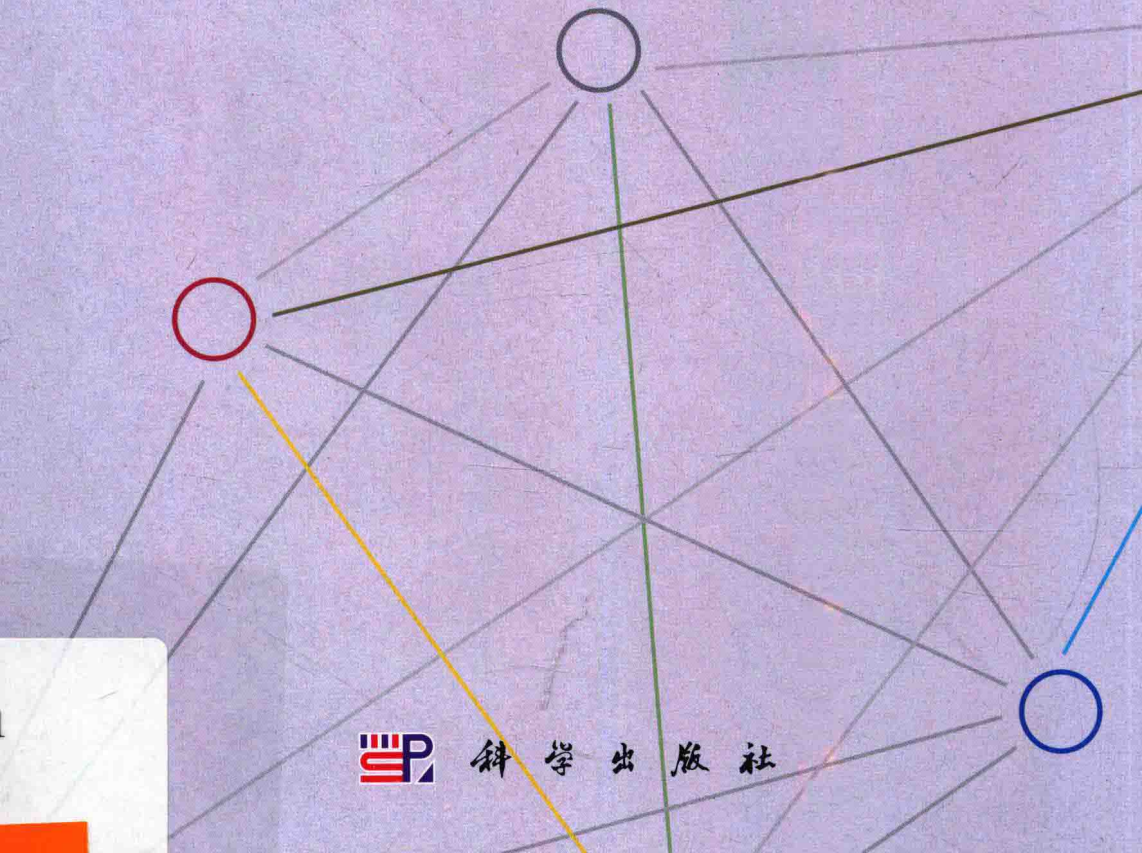
混合签密理论

俞惠芳　著



科学出版社

混合签密理论

俞惠芳 著

科学出版社

北京

内 容 简 介

混合签密由非对称的签密密钥封装机制和对称的数据封装机制组成，可以实现任意长度消息的安全通信。混合签密的非对称部分和对称部分的安全需求完全独立，可以分开研究各自的安全性。相对于公钥签密，混合签密在密码学应用中具有更高的灵活性和安全性。本书介绍几种混合签密方案及其安全结果的证明过程，其中多个成果是作者多年教学和研究的结晶。全书共 8 章，内容包括绪论、密码学基础、IBHS 方案、ES-CLHS 方案、PS-CLHS 方案、CLHRS 方案、LC-CLHS 方案、总结与展望。本书力求使读者能够直观理解每部分知识，深入理解和掌握混合签密方案的设计及证明方法。

本书既可以作为高等院校密码学、信息安全、应用数学、计算机科学、网络通信、信息科学等专业的研究生和高年级本科生的教材和参考书，也可以作为密码学、信息安全等领域工程技术人员和研究人员的参考资料。

图书在版编目（CIP）数据

混合签密理论 / 俞惠芳著. —北京：科学出版社，2018.3
ISBN 978-7-03-056840-3

Ⅰ. ①混… Ⅱ. ①俞… Ⅲ. ①密钥学 Ⅳ. ①TN918.1

中国版本图书馆 CIP 数据核字（2018）第 048831 号

责任编辑：余 丁 / 责任校对：郭瑞芝
责任印制：师艳茹 / 封面设计：蓝 正

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com
新科印刷有限公司 印刷

科学出版社发行 各地新华书店经销

*

2018 年 3 月第 一 版 开本：720×1000 1/16
2018 年 3 月第一次印刷 印张：9
字数：201 000

定价：68.00 元

（如有印装质量问题，我社负责调换）

前　言

在当今的信息时代，互联网已经渗透到社会经济、政治文化等各个领域，正不断影响着人们的工作和生活方式。各种网络服务给人们既带来了便利也带来了威胁。互联网的不断发展，促使危害信息安全的事件不断发生，敌对势力的破坏、黑客攻击、利用计算机犯罪、有害内容泛滥、隐私泄露等对信息安全构成了极大威胁。信息的存储、传输和处理越来越多地在开放网络上进行，极易遭受到各种网络攻击的威胁。由此可见，信息安全已经成为信息社会亟待解决的最重要问题之一。在全球信息化迅速发展的今天，开展信息安全研究，增强信息安全技术，提高信息安全风险的认识和基本防护能力，营造信息安全氛围，是时代发展的客观要求。

密码技术是保障信息安全的关键技术。最常用的密码技术是加密和签名。加密可以使任何非授权者不能得到消息内容，签名可以使接收者能够确定消息的发送者是谁。随着信息安全的快速发展，人们对网络传输的数据安全性要求越来越高，同时对保密性和认证性的需求也越来越广泛。这种情况说明加密或签名的单独使用已经远远不能满足人们的需求，实际应用中往往需要整合加密和签名。签密技术是公认的能同时实现签名和加密的理想方法。现有大多数签密方案都是在使用公钥认证方法的情况下同时实现加密和签名过程，这样使得被传输的消息取自某个特定集合，使其应用范围受到限制。

混合签密由签密密钥封装机制（KEM）和数据封装机制（DEM）两部分组成，可以实现任意长度消息的安全通信。签密 KEM 运用公钥技术封装一个对称密钥，DEM 使用对称技术加密任意消息。混合签密允许签密 KEM 和 DEM 的安全需求完全独立，可以分别研究各自的安全性。密码学是信息安全的核心和基础，混合签密是密码学中较为新颖的一种密码原语。近年来，混合签密的设计方法、设计工具及安全性证明都得到了扩展和深化。混合签密在电子邮件收发、在线电子交易、在线电子服务等方面有着广泛应用，利用混合签密可以确保交易双方的安全性，降低商业风险。

业内预测，五年后全球范围内网络空间安全人才缺口将达到 350 万。相对于我国庞大的上网人数、迅猛发展的网络经济规模和严峻的全球网络安全形势，为网络空间安全护航的人才队伍尤显匮乏，所以加快培养适应社会需求、多类型、多层次的高素质网络空间安全人才迫在眉睫。为了适应网络空间安全发展

的需求，作者撰写了本书。

本书在阐述混合签密内容的时候，主要采用描述性的方式向读者介绍混合签密理论研究的最新成果，作者力图使本书成为一本在密码学与信息安全领域对读者提供帮助、缩短熟悉最新理论时间的参考书。

本书是混合签密理论方面的最新专业著作，是作者近几年从事包括混合签密理论及安全性证明方法在内的密码学与信息安全学的教学和科研成果的总结。本书可供从事混合签密理论研究和技术开发的人员参考使用，也可以作为网络空间安全、通信工程、软件工程、网络工程、信息对抗技术、计算机科学与技术等专业的研究生及高年级本科生的教材和参考书。

在本书付梓之际，特别感谢我的导师——陕西师范大学计算机科学学院博士生导师杨波教授，书中包含的部分成果是作者攻读博士学位期间在杨老师的悉心指导和科研课题支持下取得的。由衷感谢西北师范大学计算机科学与工程学院的王彩芬教授、西安邮电大学自动化学院的王之仓教授和青海交通职业技术学院信息工程系的廖春生教授，他们为本书提出了许多建设性意见。也感谢李建民、高新哲、付帅凤、张杰、罗海秀等五名同学的帮助。

本书受到国家自然科学基金项目（61363080, 61572303, 61772326）和青海省基础研究计划项目（2016-ZJ-776, 2015-ZJ-718）的资助。

由于密码学的创新层出不穷，整合对称密码和公钥密码的研究越来越多，混合签密理论日新月异，研究文献汗牛充栋，故本书不足之处在所难免，敬请读者批评指正。您的建议和意见是作者前进的方向和动力，作者会及时做出答复和改进。作者的联系方式：yuhuifang@qhnu.edu.cn。

目　录

第1章 绪 论

1.1 研究背景和意义

习总书记在2014年2月27日中央网络安全和信息化领导小组第一次会议上指出：没有网络安全就没有国家安全，没有信息化就没有现代化。不强化网络化的信息安全保障，不解决信息安全问题，则信息化不可能持续、健康发展，与之相关的经济安全、政治安全、国家安全也不可能得到可靠保障。

1.1.1 信息安全的重要性

信息安全的保障能力是21世纪经济竞争力、生存能力和综合国力的重要组成部分。信息安全可抵御信息侵略和对抗霸权主义。信息既是战略资源也是决策之源，信息必须是安全可信的，如果信息不安全了，错误的信息将会起到非常大的反作用。发达国家将信息对抗与争夺作为国家与国家之间斗争的主要方式。若解决不好信息安全问题，国家则会处于信息战、信息恐怖和经济风险等威胁之中[1,2]。

信息化社会的人们从事政治、经济、军事、外交、文化、商业、金融、社会生活等各项活动时往往需要借助于互联网，这使人们无时无刻不面临各种信息安全威胁[3-5]。信息技术的发展推动了军事革命，出现了信息战法、网络战法等新型战法及网军等新型军兵种。两次海湾战争和科索沃战争中，美国都成功实施了信息作战。2010年美国和以色列利用计算机病毒成功攻击伊朗核工厂，毁坏了大部分的铀离心机，重挫了伊朗的核计划。2013年斯诺登引爆棱镜门事件。2015年雅虎证实超15亿用户信息遭窃，同年希拉罗里邮件门事件曝光。2015年中国团队360Vulcan在黑客大赛中仅用1秒就成功攻破被称为史上最难攻破的IE浏览器。2017年Dun & BrandStreet的52GB的数据库遭泄露，这套数据库包括美国数千家公司员工和政府部门的约3380万个电子邮件地址和其他联系信息，在美国影响范围巨大。现如今，信息安全问题日益突出，信息安全威胁的事件频繁在网络和电视等媒体报道，信息安全的形势不容乐观，已经严重威胁到了人们的正常生活甚至国家安全。信息安全问题是影响国家大局和长远利益的亟待解决的重大关键问题。在信息技术应用过程中，信息是最宝贵的资源，互联网为获取信息和传播信息提供了极大的便利。互联网可以使人们不受

空间和时间的限制与世界任何角落的个人或组织进行信息交流，而且每天发生的各种重大事件都能以最快速度向全世界传播。

什么是信息安全（Information Security）呢？信息安全是指计算机信息系统的硬件、软件、网络及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。信息安全的基本属性表现在以下几个方面：

（1）保密性（Confidentiality）。保密性是指确保信息不暴露给未授权的实体或进程。

（2）数据完整性（Data Integrity）。数据完整性是指只有得到授权的实体才能修改数据，并且能够辨别数据是否已被修改。

（3）可用性（Availability）。可用性是指得到授权的实体在需要时可以访问数据，即攻击者不能占用所有资源而阻碍授权者的工作。

（4）可控性（Controllability）。可控性是指可以控制授权范围内的信息流向、信息传播、信息内容等，信息资源的访问是可以控制的，网络用户的身份是可以验证的，用户活动记录是可以审计的。

（5）不可否认性（Non-repudiation）。不可否认性是指防止通信中的任何一方否认它过去执行过的某个操作或者行为。

然而，目前信息安全面临着许多自然的或人为的威胁。一般来说，自然威胁是指来自各种自然灾害、恶劣的电磁辐射或电磁干扰、网络设备老化等。这些事件有时会直接影响信息的存储介质，威胁信息的安全。人为威胁包括信息泄露、破坏信息的完整性、拒绝服务、非授权访问、窃听、业务流分析、假冒、旁路控制、授权侵犯、抵赖、信息安全法律法规不完善等。常见的信息安全威胁如图 1-1 所示。

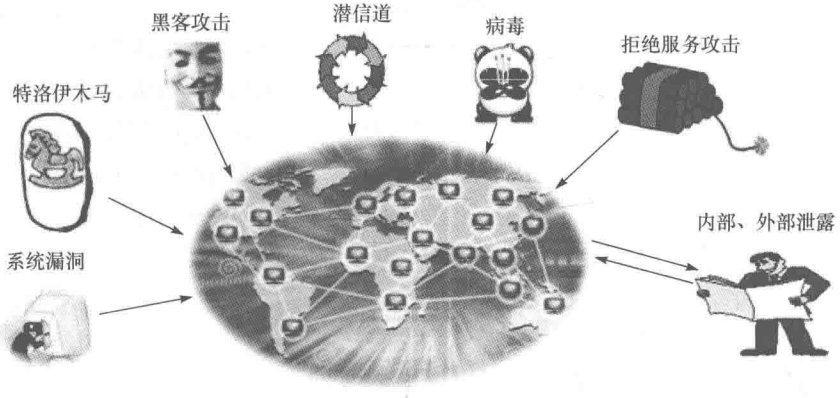


图 1-1　常见的信息安全威胁

1.1.2　密码理论

信息安全是一门涉及计算机、网络、信息论、密码学、电子、通信、数学、物理、生物、管理、法律、教育等的综合性学科，主要研究确保信息安全的科学与技术。密码学是信息安全的核心和基础，在信息安全领域有着重要地位和作用。离开了密码学，信息安全将无从谈起。

密码学包含密码编码学（Cryptography）和密码分析学（Cryptanalysis）两个分支。密码编码学主要研究对信息进行编码，以保护信息在传递的过程中不被敌手窃取、解读和利用。密码分析学主要研究通过密文获取对应的明文信息，即在未知密钥的情况下从密文推导出明文或密钥的技术。密码编码学和密码分析学既相互对立又相互依存，从而推动了密码学自身的快速发展[6-11]。

在密码学中，用来提供信息安全服务的原语称作密码系统（Cryptosystem）。根据密码系统所使用的密钥，密码系统可以分为对称密码系统（Symmetric Cryptosystem）和非对称密码系统（Asymmetric Cryptosystem）。对称密码系统又称单钥密码系统（One-Key Cryptosystem）或私钥密码系统（Private Key Cryptosystem），特点是加密和解密的密钥相同，密钥保密不公开。对称密码系统模型如图 1-2 所示。

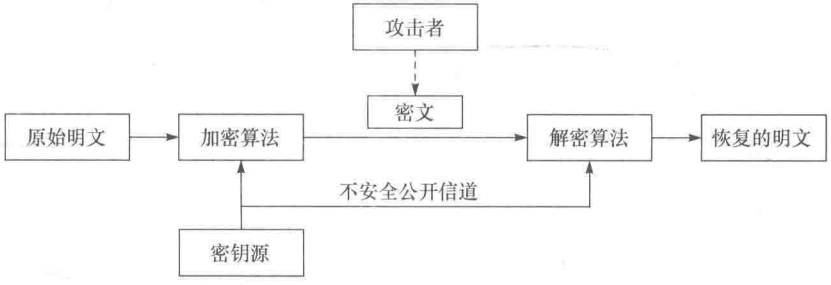


图 1-2　对称密码系统模型

公钥密码出现之前，对称密码系统的安全性基于私钥和加密算法的保密。对称密码系统的代价昂贵，故而密码学主要用于军事、政府和外交等机要部门。在对称密码系统中，加密密钥和解密密钥是相同的，通常使用的加密算法简单高效、密钥短、安全性高。但是传送和保管密钥是严峻问题。

1976 年，Diffie 和 Hellman 发表的论文《密码学的新方向》是公钥密码诞生的标志，即发送者和接收者之间不需要传递密钥的保密通信是可能的。公钥密码使密码学发生了一场变革，在密码学发展史上具有里程碑意义。公钥密码系统（Public Key Cryptosystem）又称双钥密码系统（Two-Key Cryptosystem），实质上就是非对称密码系统。公钥密码系统解决了对称密码系统中最难解决的密

钥分配和数字签名两个问题，特点是加密密钥（或公钥）和解密密钥（或私钥）是不同的。公钥密码系统模型如图 1-3 所示。

为了适应高度网络化和信息化的社会发展需求，密码学研究从消息加密扩展到数字签名、消息认证、身份识别、防否认等新领域。事实上，网络上应用的信息安全技术，比如数据加密技术、数字签名技术、混合签密技术、网络编码技术、多方安全计算技术、区块链技术、抗量子计算攻击的密码技术、消息认证技术、身份识别技术、反病毒技术、防火墙技术等都是使用密码学理论设计的。如今密码学应用非常广泛，各国政府都十分重视密码学的研究和应用。

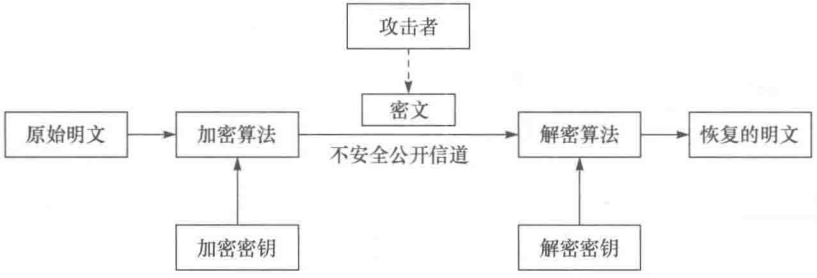


图 1-3　公钥密码系统模型

1.1.3　签密技术

密码系统可使通信各方在不安全的信道中安全地传输信息。保密性和认证性是密码学提供信息安全服务的重要内容，是签密体制形式化定义的基本安全概念。机密性可以保证信息只为授权用户使用，不能泄露给未授权的用户。认证性可以防止通信方对以前的许诺或者行为否认。保密性通过加密实现，加密可以使可读的明文信息变换为不可读的密文信息。认证性通过签名实现，签名可以使数据的接收者确认数据的完整性和签名者的身份。随着信息技术的迅速发展，仅仅靠加密是不能满足密码学应用的安全需求。如果加密密文在网络传输过程中被篡改，接收者即使使用正确的密钥解密也不能获得正确消息；同时发送者的身份认证也是非常重要的问题。由此可见，加密或签名单独使用是远远不够的，密码学应用中往往要将加密和签名整合使用[12]。

同时提供保密性和认证性两个安全目标的传统方法是“先签名后加密”，其计算量和通信成本是加密和签名的代价之和，计算效率低。签密（Signcryption）[13]是整合加密和签名的代表性密码协议，其计算量和通信成本都要低于传统的“先签名后加密”方法。签密简化了同时需要保密与认证的密码方案的设计，合理设计的签密方案可取得更高的安全水平，任何能够同时提供保密性与认证性的公钥密码方案均可以归到签密的范畴。许多学者对签密的工作原理进行了深入的研究，设计了不少具有特性的安全高效的签密方

案[14-24]，这些研究成果表明签密在密码学应用领域中可以提供信息保密、身份认证、权限控制、数据完整性和不可否认等安全服务。由于签密技术的广泛应用和迅速发展，2011 年 12 月 15 日国际标准化组织正式将签密列为安全技术的标准（ISO/IEC 29150）。

公钥密码[25]是密码学的核心技术，可是公钥密码函数运行在很大的代数结构中，计算代价昂贵。对称密码函数却具有更高的运行效率，而且对消息长度没有任何限制，在任意长度数据需要安全的时候，对称密码经常被使用。因此，在密码学应用中需要任意长度数据安全的时候，混合密码系统（Hybrid Cryptosystem）应运而生了。混合密码系统是对称密码和公钥密码的简单组合，也可以看作是公钥密码系统的一个分支，混合密码系统的重要标志是 KEM-DEM 结构[26]。KEM-DEM 结构将混合加密分为 KEM（Key Encapsulation Mechanism）和 DEM（Data Encapsulation Mechanism）两个独立的组件，各组件的安全性可以分开研究。KEM 与公钥加密类似，不同的是通过 KEM 算法生成的是对称密钥和对该对称密钥的加密密文，而不是消息的加密密文。DEM 与对称加密类似，只是 DEM 用的加密密钥是由 KEM 算法随机产生的对称密钥。混合密码系统目前已经受到了各个制定未来公钥密码标准组织的高度重视，比如 ISO 要求所有候选加密方案都应该能够加密任意长度的消息，从而必须适用于混合加密[27]。

签密有公钥签密（Public Key Signcryption）和混合签密（Hybrid Signcryption）两类。公钥签密所处理的消息取自某个特定集合，这样不能实现大消息的安全通信。为了解决任意长度的消息的保密并认证的通信问题，在 KEM-DEM 结构的理论基础上许多混合签密[28-35]被设计。混合签密由签密 KEM 和 DEM 两部分组成，其中签密 KEM 在发送者私钥和接收者公钥共同作用下生成对称密钥和对称密钥封装，DEM 则利用对称密钥加密任意长度的消息。类似于混合加密，可以分开研究签密 KEM 和 DEM 的安全性。混合签密的优势在于对消息长度没有限制、设计灵活、运算效率高。混合签密是同时实现保密并认证的重要手段，而且安全性越来越完善。混合签密的工作过程如图 1-4 所示，图中 S_a 和 S_b 分别表示发送者和接收者的私钥，P_a 和 P_b 分别表示发送者和接收者的公钥。

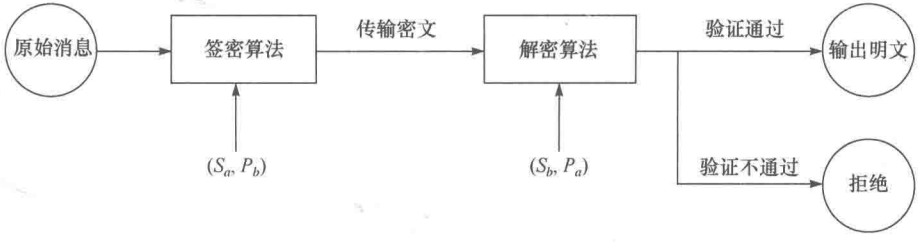


图 1-4　混合签密的工作过程

1.1.4　混合签密分类

传统的公钥基础设施（Public Key Infrastructure，PKI）采用证书管理公钥，通过可信第三方认证中心（Certificate Authority，CA）把用户公钥和用户的其他标识信息捆绑在一起，在互联网上验证用户的身份。CA 的功能有证书发放、证书更新、证书撤销和证书验证，CA 还要负责用户证书的黑名单登记和黑名单发布。公钥证书是一个结构化的数据记录，包括用户的身份信息、公钥参数和证书机构的签名等。任何人都可以通过验证证书的合法性来认证公钥。如果一个用户信任认证机构，则该用户验证了另一用户证书的合法性之后，就应该相信公钥的真实性。PKI 使用任何公钥都要事先验证公钥证书的合法性，增加了用户的计算量。PKI 的运行过程：用户向注册中心（Registration Authority，RA）提交证书申请或证书注销请求，由 RA 审核。RA 将审核后的用户证书申请或证书注销请求提交给 CA。CA 最终签署并颁发用户证书并且登记在证书库中，同时定期更新证书注销列表（Certificate Revocation List，CRL），供用户查询。从根 CA 到本地 CA 存在一条链，下一级 CA 由上一级 CA 授权。CA 还可能承担密钥备份和恢复工作。PKI 运行模型如图 1-5 所示，CA 运行模型如图 1-6 所示。图 1-5 中 LDAP（Lightweight Directory Access Protocol）是指轻量级目录访问协议。

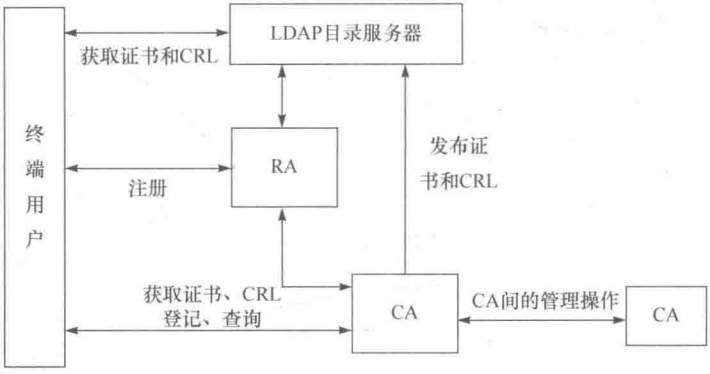


图 1-5　PKI 运行模型

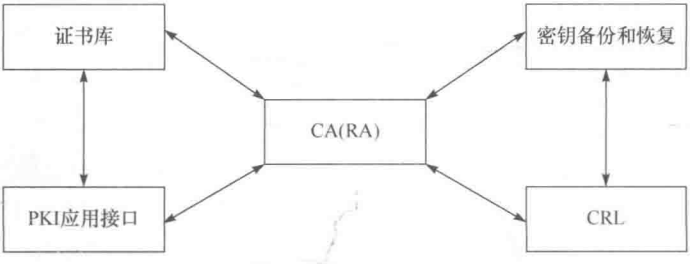


图 1-6　CA 运行模型

Shamir在1984年提出了基于身份的公钥密码系统（Identity-Based Public Key Cryptosystem，IB-PKC）[36]的思想，简化了传统的PKI公钥体系架构中的CA对各用户证书的管理，其基本的想法就是用户公钥由用户的公开身份信息确定，私钥生成器（Private Key Generator，PKG）利用用户的公开身份信息计算出用户私钥。在IB-PKC中，当一个用户使用另一个用户的公钥时，只需要知道该用户的身份信息，而不需要去获取和验证该用户的公钥证书。由此可见，IB-PKC减少了公钥证书的存储、颁发、撤销及公钥验证费用。然而，PKG知道所有用户的私钥，可以冒充任何用户进行任何密码操作且不被发现，这使得IB-PKC无法避免密钥托管问题。

为了克服传统的PKI中的证书管理问题和IB-PKC中固有的密钥托管问题，Al-Riyami和Paterson[37]在2003年提出了无证书公钥密码系统（Certificateless Public Key Cryptosystem，CL-PKC）。在CL-PKC中，用户的完整私钥由密钥生成中心（Key Generation Center, KGC）产生的部分私钥和用户自己随机选取的秘密值两部分组成，用户公钥是用户自己计算得到的。CL-PKC不再使用证书对用户公钥和用户身份进行绑定，也不需要托管密钥，因而在实际网络中有着广泛的应用前景。

目前认证公钥的方法有基于PKI的公钥密码体制、基于身份的公钥密码体制和基于无证书的公钥密码体制三种。Girault[38]定义了下面三个信任标准。

信任标准1：认证机构知道或可以轻松得到用户私钥，因而可以冒充用户并且不被发现。

信任标准2：认证机构不知道或不能轻松得到用户私钥，但是仍然可以产生一个假的证书冒充用户并且不被发现。

信任标准3：认证机构不知道或不能轻松得到用户私钥，如果认证机构生成一个假的证书冒充用户，他将被发现。

从三个信任标准可以看出，基于PKI的公钥密码体制达到了信任标准3，因为同一个用户拥有两个合法的证书则意味着认证机构的欺骗；基于身份的公钥密码体制只达到了信任标准1，因为PKG知道所有用户的私钥；基于无证书的公钥密码体制达到了信任标准3并且不需要公钥证书。

根据公钥认证方法的不同，混合签密方案可以分为基于PKI的混合签密方案、基于身份的混合签密方案和基于无证书的混合签密方案。将混合签密体制和具有特殊性质的数字签名相结合，可以设计具有特殊性质的混合签密方案，比如将混合签密体制与环签名集成在一起则可以形成混合环签密体制。本书接下来的大部分内容主要描述不同公钥认证的混合签密方案及其可证明安全性。

1.2　国内外研究现状

电子商务、电子政务及日常生活网络化与信息化，使得信息安全的核心和基础技术——密码学技术得到了很大发展。在任意长度的数据需要保密并认证通信的密码学应用需求下，使用密码学技术的不同公钥认证的混合签密技术具有了良好的应用前景。这也说明目前公钥签密技术在很多情形下已经不能满足密码学应用需求，在现实场景中往往需要处理任意长度的消息以适用于保密并认证的不同应用环境。在这样的应用背景下，不同公钥认证的混合签密技术就在混合密码系统的理论研究基础之上发展起来了。

混合签密技术的研究最先是从混合加密技术着手的。混合加密起初是先用公钥加密方案加密对称密钥，再用该对称密钥加密真正的消息，此时的混合加密仅仅限于密码学应用需求，并没有形式化安全定义。直到 2004 年，Cramer 等对混合加密的 KEM-DEM 结构进行了形式化安全定义[27]。混合加密[39-43]的优势是可以实现任意长度的消息的安全保密通信。混合加密由完全独立的 KEM 和 DEM 两部分组成，KEM-DEM 结构允许分别定义 KEM 与 DEM 的安全需求。为了使得整个混合加密达到某种安全水平，只要 KEM 和 DEM 分别达到相应的安全水平即可，这极大方便了混合结构的安全性分析。

Dent 在 2005 年使用 KEM-DEM 结构设计了一个内部安全的混合签密方案[44]和一个外部安全的混合签密方案[45]，给出了相应的混合签密方案的算法模型和形式化安全定义。目前混合签密[28-35,46-51]是密码学界的一个重要研究方向，其非对称部分签密 KEM 需要接收者的公钥和发送者的私钥作为输入，从而确保了所产生随机密钥的数据完整性，起到了数字签名的效果；然而，其对称部分 DEM 使用非对称部分产生的对称密钥加密任意长度的消息，保证了消息确确实实源自于所声称的消息源。

密码学界主要研究了基于 PKI 的混合签密方案、基于身份的混合签密方案和无证书混合签密方案。混合签密可以应用于网上报关、网上报检、网上办公、网上采购及网上报税等电子政务和电子商务系统，也可以应用于电子支付、电子邮件、数据交换、电子货币及物联网等领域。在电子签章系统中，只有合法拥有印章钥匙盘并且有密码权限的用户才能在文件上加盖电子签章；而且可以通过密码验证、签名验证、数字证书等验证身份的方式验证用户的合法性，可以查看和验证数字证书的可靠性。

相比较于公钥签密技术，混合签密技术具有更高的效率和更好的灵活性，尤其是在要求大量数据保密并认证通信的情形下。目前混合签密技术在网络通

信中起着重要作用。如何设计使用不同公钥认证方法的具有不同特性的混合签密方案及如何证明所设计方案的安全性，仍然没有完成，还在继续进行和完善之中。针对混合签密理论的研究及讨论方兴未艾。混合签密是公钥密码的一个扩展，也是一种重要的密码学技术。混合签密理论看似简单，但是根据密码学界的不同研究目的或者结合密码学中其他一些技术，混合签密技术的实现方式却又丰富多彩。混合签密被提出至今十几年的时间里，不断地沿着不同方向延伸和发展。混合签密方案的设计及其可证明安全性理论的研究工作还需要进一步完善和创新。

虽然目前已经公布了不少使用不同公钥认证方法的混合签密理论方面的研究结果，但是设计安全性强、计算复杂度低和通信效率高的混合签密方案仍具有重要的理论意义和实际价值。本书重点是在椭圆曲线离散对数问题、椭圆曲线计算 Diffie-Hellman 问题、椭圆曲线判定 Diffie-Hellman 问题、双线性 Diffie-Hellman 问题、计算 Diffie-Hellman 问题、双线性判定 Diffie-Hellman 问题、联合双线性 Diffie-Hellman 问题、联合计算 Diffie-Hellman 问题、联合判定双线性 Diffie-Hellman 问题等的理论基础之上，说明如何去设计实用的基于身份的混合签密（Identity-Based Hybrid Signcryption，IBHS）方案，使用三个乘法循环群的高效安全的无证书混合签密（Efficient and Secure Certificateless Hybrid Signcryption，ES-CLHS）方案、可证明安全的无证书混合签密（Provably Secure Certificateless Hybrid Signcryption，PS-CLHS）方案、基于无证书的混合环签密（Certificateless Hybrid Ring Signcryption，CLHRS）方案和低计算复杂度的无证书混合签密（Low-Computation Certificateless Hybrid Signcryption，LC-CLHS）方案，进而说明如何在随机预言模型中采用归约的方法证明这些密码方案的安全性及如何给出其概率分析过程。

在安全性证明中，随机预言模型通常是现实中哈希函数的理想化替身。哈希函数是一个输入为任意长度，输出为固定长度的函数，除此之外还满足单向性、抗碰撞性等。在随机预言模型下通常证明所设计的密码方案是安全的；而在密码方案的实际执行的时候，用具体的哈希函数来替换密码方案中的随机预言机。在标准模型下敌手只受时间和计算能力的约束，而没有其他假设；在标准模型下的可证明安全性可以将密码方案归约到困难问题上。然而在实际中，很多密码方案在标准模型下建立安全性归约是比较困难的，也就是难于证明在安全模型下的安全性。因此，为了降低证明的难度及计算复杂度，往往在安全性归约过程中加入其他假设条件。

随机预言模型中的安全性证明除了散列函数外的环节都可达到安全要求，目前大多数的可证明安全混合签密方案也是基于随机预言机模型的。因此，随机预言机模型仍然被认为是混合签密方案的可证明安全中最成功的应用。本书的