密码工程学

李浪 邹祎 郭迎 编著

清华大学出版社

密码工程学

李浪 邹祎 郭迎 编著

清华大学出版社
北京

内 容 简 介

密码算法的实现及其优化是非常重要的一门工程技术科学，是信息安全的重要组成部分。本书从密码算法的软硬件实现及其优化的角度进行论述，内容包括密码算法实现的基础技术、分组密码原理与实现技术、公钥密码原理与实现技术、序列密码原理与实现技术、Hash 函数实现原理与技术、数字签名实现原理与技术。本书也重点论述了适应目前资源约束物联网环境下的轻量级密码算法原理与优化实现技术，包括典型轻量级密码算法优化的实现方法，轻量级密码算法的设计原理与方法，并以作者提出的 Magpie 轻量级密码算法为例进行设计方法学的介绍，以经典的 DES 和 AES 密码算法为例介绍密码算法 FPGA 的实现方法。最后，论述了密码芯片的主要攻击与防御技术。为了方便读者更好地掌握密码算法的实现技术，以附录的形式给出了 6 个密码算法的实验教程，方便学习者进行实际训练。

本书部分内容是作者长期在密码领域内研究的最新成果，以初学者的角度进行内容编写，特别适合计算机、通信、物联网、网络工程、软件工程、电子商务、信息安全、信息管理等专业的学生进行入门学习，强调学习者动手能力的培养。同时，可供相关专业的研究生作为学习教材，也适合相关工程技术领域的科技人员作为参考。

图书在版编目(CIP)数据

密码工程学/李浪，邹祎，郭迎编著. —北京：清华大学出版社，2014
ISBN 978-7-302-37968-3

Ⅰ. ①密…　Ⅱ. ①李… ②邹… ③郭…　Ⅲ. ①密码—理论　Ⅳ. ①TN918.1

中国版本图书馆 CIP 数据核字(2014)第 209531 号

责任编辑：张　民　薛　阳
封面设计：傅瑞学
责任校对：梁　毅
责任印制：沈　露

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 装 者：北京国马印刷厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：15.75　　**字　　数**：392 千字
版　　次：2014 年 12 月第 1 版　　**印　　次**：2014 年 12 月第 1 次印刷
印　　数：1～2000
定　　价：34.50 元

产品编号：059819-01

前言

信息安全在当代信息社会无比重要，密码是信息安全的基石。社会需要大批的信息安全人才，一本好的密码学教材显得非常重要。

作者多年从事信息安全研究与教学，发现目前特别需要一本既汇聚密码学基础，又能体现密码算法与硬件优化实现，同时又能有最新密码技术的书籍。本书能够让读者阅读之后，快速入门并迅速掌握密码软硬件的实现技术，能够对密码算法安全设计有所思考。

对常见的密码算法原理及其实现技术进行了概括性提高，对目前适合资源约束的新型轻量级分组密码算法进行了优化实现，并以有自主知识产权的 Magpie 轻量级密码算法为例，结合设计方法学论述了轻量级密码算法的设计理念。密码算法及其芯片仍然是攻击者的重点攻击对象，论述了主要攻击技术及其防御方法。有些内容是作者的最新研究成果，还有一些内容是作者博士期间的研究工作。

本书的主要特点是：以初学者的角度进行论述、强调基础、注重实践操作能力的培养，力求使学习者在掌握密码算法基本原理的基础上，能够对密码设计与优化方法有所掌握，特别是对硬件语言实现及密码算法优化有较深的理解，对目前密码算法的主要攻击技术及其防御方法有所掌握。

本书主要由李浪教授负责编写与组织统稿，其中李浪负责编写第 1～第 6 章、第 8 章和第 10.1、第 10.2、第 10.5 节，邹祎负责编写第 7 章与第 10.4 节，许琼方负责编写第 10.3 节，王玉奇对目录和内容架构提出了宝贵意见，中南大学郭迎博士对相关章节进行了详细的校对，同时提出了许多建设性的意见。特别值得指出的是，李浪教授负责的嵌入式计算与信息安全研究所的刘波涛、余孝忠、曾婷、杜国权、李配对本书的附录进行了编写，并为全书进行了大量的基础性工作，如对程序源码及其实现都进行了认真的实验与校对。本书的编写得到了清华大学出版社张民老师的大力支持，同时一些基础性原理与内容参考了大量同行的相关著作与教材，在参考文献中也进行了注明，作者在此一并表示感谢。

本书获得了湖南省普通高等学校教学改革研究项目“基于协同创新的地方本科院校计算机专业应用人才培养研究”的资助(NO. 2014382)。

尽管作者以最大的努力去编著本书，但由于作者的学识和水平毕竟有限，特别是书中有些内容是作者教学与科研中的原创成果，因此难免有需要商榷之处，诚望读者不吝赐教斧正，作者的电子邮箱是：lilang911@126.com。

本书制作了配套的电子课件，方便使用本书的老师进行教学使用，课件可从清华大学出版社网站 http://www.tup.tsinghua.edu.cn 下载，也可联系作者索取。

李　浪

2014 年 5 月

目录

第1章 绪 论

本章首先从信息安全的角度引入密码工程学的重要性，介绍密码技术的发展过程，包括古代密码、近代密码和现代密码；同时，介绍了密码工程学中的一些基本概念，强调了密码工程学的主要任务和最新进展。

1.1 信息安全与密码技术

1.1.1 信息安全简述

进入21世纪，随着互联网的快速发展，人类社会对信息的依赖程度越来越大，对信息安全也越来越关注，同时随着应用与研究的深入，使得信息安全的概念与技术不断得到创新。在计算机网络广泛使用之前主要是开发各种信息保密技术，Internet在全世界商业化应用之后，信息安全进入网络信息安全阶段。其最根本的属性是防御性，主要目的是防止信息的完整保密及可用性遭到破坏。

一般来讲，信息安全主要包括系统安全及数据安全两方面的内容。系统安全一般采用防火墙、病毒查杀、防范等被动措施；而数据安全主要采用现代密码技术对数据进行主动保护，如数据加密、数据完整性、数据不可否认与抵赖、双向身份认证等。信息安全的概念与技术是随着人们的需求以及计算机、通信与网络等技术的发展而不断发展的，大体可分为信息保密、网络信息安全和信息保障三个阶段。

1）信息保密阶段

信息保密阶段的研究成果主要有两类：发展各种密码算法及其应用；计算机信息系统保密模型和准则。

2）网络信息安全阶段

在此阶段，除了采用和研究各种加密技术外，还开发了许多针对网络环境的信息安全与防护技术，这些防护技术是以被动防御为特征的，大体分为以下几种。

（1）安全漏洞扫描器。

用于检测网络信息系统是否存在漏洞，并提供相应的解决方案。

（2）安全路由器。

在普通路由器的基础上增加更强的安全过滤规则，增加认证与防瘫痪性攻击的各种措施。安全路由器完成在网络层与传输层的报文过滤功能。

（3）防火墙。

在内部与外部网的入口处安装的堡垒主机，在应用层利用代理功能实现对信息流的过滤功能。

（4）入侵检测系统。

根据已知的各种入侵行为的模式判断网络是否遭到入侵的一类系统，一般也具备告警、审计与简单的防御功能。

(5) 网络监控与审计系统。

监控内部网络中的各种访问信息流,并对指定条件的事件做审计记录。各种防网络攻击技术,其中包括网络防病毒、防木马、防口令破解、防非授权访问等。

3) 信息保障阶段

信息保障的概念最初是由美国国防部长办公室提出来的。信息保障(Information Assurance)的定义为:通过确保信息和信息系统的可用性、完整性、可验证性、保密性和不可抵赖性来保护信息系统的信息作战行动,包括综合利用保护、探测和反应能力以恢复系统的功能。信息保障阶段的许多内容都是战略性的,具有指导意义。

(1) 信息保障技术框架。

信息保障技术框架(Information Assurance Technical Framework),是由信息保障技术框架论坛(Information Assurance Technical Framework Forum)定义的,是一系列为保证信息安全和信息基础架构的指导方针。IATF 定义了为发展带有信息保障系统的一个过程和硬件的安全需求和在系统中的软件部件。应用这些原理导致在信息基础架构中的保护,也叫深度防护战略。

(2) 信息系统安全工程。

IATF 定义了信息系统安全工程(Information System Security Engineering)过程,用于开发一个安全的系统。ISSE 过程定义了信息系统安全的原则、活动及其与其他过程的关系。遵循这些原则,可以对信息基础设施进行名为"纵深防御战略"的多层防护。纵深防御战略的 4 个技术焦点域分别是:保护网络与基础设施、保护飞地边界、保护计算环境和支撑性基础设施。

1.1.2 密码技术简述

密码技术是保护信息安全的主要手段之一。密码技术自古有之,到目前为止,已经从外交和军事领域走向公开。随着现代计算机技术的飞速发展,密码技术正在不断向更多领域渗透。它是集数学、计算机科学、电子与通信等诸多学科于一体的交叉学科。密码技术不仅能够保证信息机密性,而且具有数字签名、身份验证、秘密分存、系统安全等功能,能够保证信息的完整性和确定性,防止信息被篡改、伪造和假冒。

1.1.3 信息安全与密码技术的关系

密码技术是实现信息安全的核心技术,是保障数据最重要的工具之一,就密码算法而言,通过加密变换,将明文打乱,从而起到保护信息和数据的作用。本书在后续章节将结合具体的密码算法来体现两者之间的关系。

1.2 密码技术发展简介

1.2.1 古代密码

1) 简介

在手工阶段,人们只需通过纸和笔对字符进行加密。人类对密码的使用可以追溯到古

巴比伦时代，图 1-1 的 Phaistos 圆盘是一种直径约为 160mm 的黏土圆盘，它始于公元前 17 世纪，表面有明显字间空格的字母。近年有研究学家认为它记录着某种古代天文历法，但真相仍是个谜。这些密码大多很简单，在实际应用中已经很少用到。这个时期的密码技术仅是一门文字变换艺术，其研究与应用远远称不上科学，最多称其为密码术。

图 1-1　Phaistos 圆盘

2）典型代表密码

恺撒密码、棋盘密码等都是古代密码的典型代表。

恺撒密码作为一种最为古老的对称加密体制，在古罗马的时候就已经很流行，它的基本思想是：通过把字母移动一定的位数来实现加密和解密。明文中所有字母都在字母表上向后（或向前）按照一个固定的数目进行偏移后被替换成密文。例如，当偏移量是 3 的时候，所有的字母 A 将被替换成 D，B 变成 E，以此类推，X 将变成 A，Y 变成 B，Z 变成 C。由此可见，位数就是恺撒密码加密和解密的密钥。

棋盘密码是利用波利比奥斯方阵（Polybius Square）进行加密的密码方式，产生于公元前 2 世纪的希腊，相传是世界上最早的一种密码。简单来说就是把字母排列好，用坐标的形式表现出来。字母是密文，明文便是字母的坐标。

1.2.2　近代密码

1）简介

近代密码的主要历程是从 20 世纪初到 20 世纪 50 年代。密码研究人员设计出采用各种各样的机电技术的转轮机来取代手工编码的加密方法，来实现保密通信的自动编解码，它是由手工或电动机械实现的复杂代替或换位，军事人员使用电报通信方式来保障信息安全。近代密码的这一阶段使得基于复杂计算的密码成为可能。

2）早期密码机

早期的密码机如图 1-2 所示。

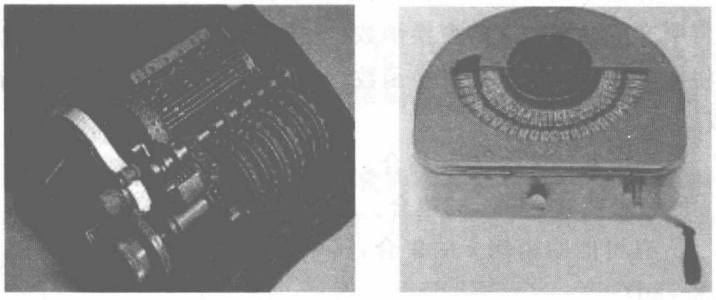

图 1-2　早期的密码机

1.2.3　现代密码

1）简介

早在 1949 年，美国人香农（Claude Shannon）发表了《保密系统的通信理论》，首次将信息论引入密码技术的研究，为现代密码学的发展奠定了坚实的理论基础，把已有数千年的密

码技术推上了科学轨道，使密码学成为一门真正的科学。人们甚至预测，当量子计算机成为现实时，经典密码体制将无安全可言，而且量子密码可能是未来光通信时代保障网络通信安全的可靠技术。现代密码的主要特点在于数据的安全是基于密钥而不是算法的保密。

2）典型代表密码

典型代表密码如对称密码 DES、AES，非对称密码 RSA、ElGamal、ECC，序列密码 RC4 算法等。本书以现代密码算法为基础，将在后续对应章节做更深入的阐述。

1.3 密码工程学的基本概念

1.3.1 密码工程学的主要任务

密码工程学是对密码算法进行实现及优化的一门技术科学，强调实践能力，在密码算法原理的基础上，强化密码算法的优化实现技术，用软件程序语言和硬件语言对密码算法进行实现，进而完成 FPGA 下载验证和 ASIC 实现。

1.3.2 密码系统的概念

1）简介

密码系统主要是用于加密与解密的系统，即明文与加密密钥作为加密变换的输入参数，经过一定的加密变换处理以后得到输出密文，在通信系统中它可能是比特流，如文本、位图、数字化的语音流或数字化的视频图像。

注意：仅用一个保密通信模型来完整描述密码系统，可能并不全面和准确，因为现在的密码系统不单单只提供信息的机密性服务。

2）基本概念与符号

明文：作为加密输入的原始信息，通常用 p 表示。

密文：是明文经加密变换后的结果，通常用 c 表示。

密钥：参与密码算法变换的参数，通常用 k 表示。

加密算法：将明文变换成密文的变换函数，变换过程简称加密，通常用 $c=E_k p$ 表示。

解密算法：将密文恢复成明文的变换函数，变换过程简称解密，通常用 $p=D_k c$ 表示。

3）系统组成

明文空间 P：所有可能的明文 p 的集合。

密文空间 C：所有可能的密文 c 的集合。

密钥空间 K：所有可能的密钥 k 的集合，其中每一密钥 k 由加密密钥 ke 和解密密钥 kd 组成，即 $k=(\mathrm{ke},\mathrm{kd})$。

加密算法 E：一簇由加密密钥控制的、从 P 到 C 的加密变换。

解密算法 D：一簇由解密密钥控制的、从 C 到 P 的解密变换。

1.3.3 对密码系统的攻击

1）攻击类型

在假设密码攻击者已知所用加密算法全部知识的情况下，根据密码攻击者对明文、密文

等数据资源的掌握程度，可将对密码系统的攻击分为4种。

(1) 唯密文攻击(Cipher Text-only Attack)。

在唯密文攻击中，密码攻击者虽知道密码算法，但仅能根据截获的密文进行分析，以得出明文或密钥。由于密码攻击者所能利用的数据资源仅为密文，这是对密码攻击者最不利的情况。

(2) 已知明文攻击(Plaintext-known Attack)。

已知明文攻击指密码分析者除了有截获的密文外，还有一些已知的“明文-密文对”来破译密码。密码攻击者的任务目标是推测用来加密的密钥或某种算法，这种算法可以对用该密钥加密的任何新消息进行解密。

(3) 选择明文攻击(Chosen-plaintext Attack)。

选择明文攻击指密码攻击者不仅可得到一些“明文-密文对”，还可以选择被加密的明文，并获得相应的密文。这时密码攻击者能够选择特定的明文数据块去加密，并比较明文和对应的密文，从中获得更多的与密钥相关的信息。密码攻击者的任务目标也是推出用来加密的密钥或某种算法，该算法可以对用该密钥加密的任何新的消息进行解密。

(4) 选择密文攻击(Chosen-ciphertext Attack)。

选择密文攻击指密码攻击者可以选择一些密文，并得到相应的明文。密码攻击者的任务目标是推导出密钥。这种密码攻击多用于攻击非对称密码体制。

2) 攻击评估

衡量密码系统攻击的复杂性主要考虑到3个方面。

(1) 数据复杂性(Data Complexity)：用做密码攻击所需输入的数据量。

(2) 处理复杂性(Processing Complexity)：完成密码攻击所需花费的时间。

(3) 存储需求(Storage Requirement)：进行攻击所需的数据存储空间大小。

1.3.4 密码系统的安全性

1) 安全因素

一个密码系统的安全性关联到两个方面。

(1) 所使用的密码算法本身的保密强度。密码算法的保密强度取决于密码设计水平、破译技术等。可以说一个密码系统所使用的密码算法的保密强度是该系统安全性的技术保证。

(2) 密码算法之外的不安全因素。因此，密码算法的保密强度并不等价于密码系统整体的安全性。一个密码系统必须同时完善技术与管理要求，才能保证整个密码系统的安全。

2) 评估方法

(1) 无条件安全性。

这种评价方法考虑的是假定攻击者拥有无限的计算资源，但仍然无法破译该密码系统。

(2) 计算安全性。

计算安全性指使用目前最好的方法攻破它所需要的计算远远超出攻击者的计算资源水平，就可以定义这个密码体制是安全的。

(3) 可证明安全性。

将密码系统的安全性归结为某个经过深入研究的数学难题(如大整数素因子分解、计算

离散对数等),数学难题被证明求解困难。这种评估方法存在的问题是它只说明了密码方法的安全性与某个困难问题相关,没有完全证明问题本身的安全性,并给出它们的等价性证明。

1.3.5 密码体制的分类

1) 根据密码算法所用的密钥数量

根据加解密算法所用的密钥是否相同,可将密码体制分为对称密码体制和非对称密码体制。

(1) 对称密码体制。

对称密码体制是一种传统密码体制,也称私钥密码体制。在对称加密系统中,加解密采用相同的密钥,同时需要通信的双方必须选择和保存他们共同的密钥,各方必须信任对方不会将密钥泄露出去,这样就可以实现数据的机密性和完整性。对于具有 n 个用户的网络,需要 $2n(n-1)/2$ 个密钥,在用户群不是很大的情况下,对称加密系统是有效的。但是对于大型网络,当用户群很大,分布很广时,密钥的分配和保存就成了问题。对机密信息进行加密和验证随报文一起发送报文摘要(或散列值)来实现。比较典型的算法有 DES、三重 DES、GDES、IDEA、FEALN、RC5 等。DES 标准由美国国家标准局提出,主要应用于银行业的电子资金转账领域,其密钥长度为 56 位。三重 DES 使用两个独立的 56 位密钥对交换的信息进行三次加密,从而使其有效长度达到 112 位。RC2 和 RC4 方法是 RSA 数据安全公司的对称加密专利算法,它们采用可变密钥长度的算法。通过规定不同的密钥长度,RC2 和 RC4 能够提高或降低安全的程度。

(2) 非对称密码体制。

非对称密码体制也叫公钥密码体制,该技术就是针对对称密码体制的缺陷被提出来的。

在公钥加密系统中,加解密是相对独立的,使用两个不同的密钥,加密密码(公开密钥)向公众公开,谁都可以使用,解密密钥(秘密密钥)只有解密人自己知道,非法使用者根据公开的加密密钥无法推算出解密密钥,故其可称为公钥密码体制。如果一个人选择并公布了他的公钥,另外任何人就都可以用这一公钥来加密传送消息。私钥是秘密保存的,只有私钥所有者才能利用私钥对密文进行解密。公钥密码体制的算法中最著名的代表是 RSA 系统,此外还有背包密码、McEliece 密码、Diffe-Hellman、Rabin、零知识证明、椭圆曲线、ElGamal 算法等。公钥密钥的密钥管理比较简单,并且可以方便地实现数字签名和验证,但算法复杂,加密数据的速率较低。公钥加密体制不存在对称加密系统中密钥的分配和保存问题,对于具有 n 个用户的网络,仅需要 $2n$ 个密钥。公钥加密体制除了用于数据加密外,还可用于数字签名,它可提供以下功能。

机密性(Confidentiality):保证非授权人员不能非法获取信息,通过数据加密来实现。

确认(Authentication):保证对方属于所声称的实体,通过数字签名来实现。

数据完整性(Data Integrity):保证信息内容不被篡改,入侵者不可能用假消息代替合法消息,通过数字签名来实现。

不可抵赖性(Non-repudiation):发送者不能事后否认他发送过消息,消息的接收者可以向中立的第三方证实所指的发送者确实发出了消息,通过数字签名来实现。

可见公钥加密系统满足信息安全的所有主要目标。

2）根据对明文信息的处理方式

可将对称密码体制分为分组密码和序列密码(也称流密码)。

(1) 分组密码。

分组密码是将消息进行分组，一次处理一个数据块元素的输入，对每一个输入块产生一个输出块。在用分组密码进行加密时，一个明文分组被当作一个整体来产生一个等长的密文分组输出。分组密码通常使用的分组长度为 64 位或 128 位。

(2) 序列密码。

序列密码则是连续地处理输出元素，一次产生一个元素的输出，在用序列密码做加密时，一次加密一个比特或一个字节。

3）根据能否进行可逆的加密变换

可将密码体制分为单向函数密码体制和双向变换密码体制。

(1) 单向函数密码体制。

这是一种特殊的密码体制，其性质是可以很容易地把明文转化为密文，但将密文转化为正确明文是不可能的。它只适合某种特殊的、不需要解密的应用场合，如用户口令存储和信息完整性保护与鉴别等。

(2) 双向变换密码体制。

双向变换密码能够进行可逆加解密变换，绝大多数加密算法都属于这一类，它要求所使用的密码算法能进行可逆双向加解密变换，否则接收者无法将密文还原成明文。另外，关于密码体制的分类还有一些其他方法，如按照在加密过程中是否引入了客观随机因素，可以分为确定型密码体制和概率密码体制等。

1.3.6　对称与非对称密码体制的主要特点

1）对称密码体制

对称密码通信模型如图 1-3 所示。

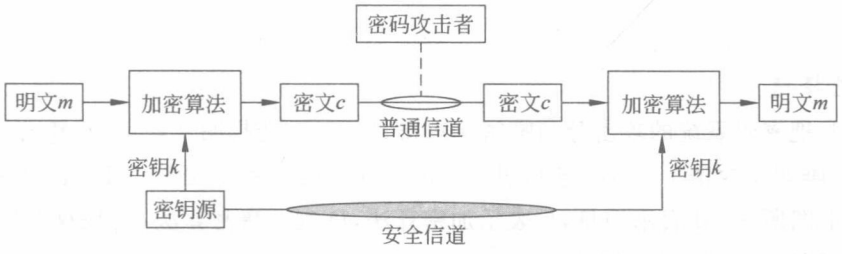

图 1-3　对称密码通信模型

(1) 主要优势。

加解密运算的处理速度快，算法安全性高。

(2) 缺陷。

对称密码算法的密码分发过程复杂，代价高；

密码管理困难；

保密通信系统开放性差；