LOIS

信息安全国家重点实验室

信息安全丛书

Quantum Cryptography

量子密码学

曾贵华 著

科学出版社
www.sciencep.com

信息安全国家重点实验室信息安全丛书

量子密码学

曾贵华 著

国家自然科学基金资助项目
（项目编号：69803008，60102001，60472018，90104005）

科学出版社

北京

内 容 简 介

本书是《信息安全国家重点实验室信息安全丛书》之一。书中深入系统地论述了量子密码的基本概念、实现原理、物理基础和信息论基础、协议与算法、密码系统的实现技术以及与经典密码的关系，并探讨了量子密码的可能应用。全书共九章，构建了量子密码的整体框架体系。主要内容包括密码学及量子密码的概况、量子比特的数学性质和物理性质、量子密钥、量子密码体制、量子认证、量子秘密共享、量子安全协议、量子密码分析、量子密码系统的实现技术及典型量子密码系统的介绍。

本书可作为密码学、物理学、量子光学、计算机科学、通信和数学等学科的科研和工程技术人员的参考书，也可供相关专业的高校师生参考。

图书在版编目(CIP)数据

量子密码学/曾贵华著. —北京：科学出版社，2006

（信息安全国家重点实验室信息安全丛书）

ISBN 7-03-017276-0

Ⅰ. 量… Ⅱ. 曾… Ⅲ. 量子-密码-理论 Ⅳ. TN918. 1

中国版本图书馆 CIP 数据核字（2006）第 051269 号

责任编辑：鞠丽娜 刘亚军/责任校对：柏连海

责任印制：吕春珉/封面设计：王 浩

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

铭浩彩色印装有限公司 印刷

科学出版社发行 各地新华书店经销

*

2006 年 6 月第 一 版 开本：B5（720×1000）

2006 年 6 月第一次印刷 印张：18 1/2

印数：1—3 500 字数：368 500

定价：35. 00 元

（如有印装质量问题，我社负责调换〈环伟〉）

销售部电话 010-62136131 编辑部电话 010-62138978-8002

《信息安全国家重点实验室信息安全丛书》编委会

序　言

人类的进步得益于科学研究的突破、生产力的发展和社会的进步。

计算机、通信、半导体科学技术的突破，形成了巨大的新型生产力。数字化的生活方式席卷全球。农业革命、工业革命、信息革命成为人类历史生产力发展的三座丰碑。古老的中华大地，也正在以信息化带动工业化的国策下焕发着青春。电子政务、电子商务的各种信息化应用之花，在华夏沃土上竞相开放，炎黄子孙们，在经历了几百年的苦难历程后，在国家崛起中又迎来了一个运用勤劳和智慧富国强民的新契机。

科学规律的掌握，非一朝一夕之功。治水、驯火、利用核能都曾经经历了非常漫长的岁月。不掌握好科学技术造福人类的一面，就会不经意地释放出它危害人类的一面。

生产力的发展，为社会创造出许多新的使用价值。但是，工具的不完善，会限制这些使用价值的真正发挥。信息化工具也和农业革命、工业革命中人们曾创造的许多工具一样，由于人类认识真理和实践真理的客观局限性而存在许多不完善的地方，从而形成信息系统的漏洞，造成系统的脆弱性，在人们驾驭技能不足的情况下损害着人们自身的利益。

世界未到大同时，社会上和国际间存在着竞争、斗争、战争和犯罪。传统社会存在的不文明、暴力，在信息空间也同样存在。在这个空间频频发生的和被有些人利用系统存在的脆弱性运用其“暴智”来散布计算机病毒，制造拒绝服务的事端，甚至侵入他人的系统，盗窃资源、资产，以达到其贪婪的目的。人类运用智慧开拓的信息疆土正在被这些暴行蚕食破坏着。

随着信息化的发展，信息安全成为全社会的需求，信息安全保障成为国际社会关注的焦点。因为信息安全不但关系国家的政治安全、经济安全、军事安全、社会稳定，也关系到社会中每一个人的数字化生存的质量。

信息革命给人类带来的高效率和高效益是否真正实现，取决于信息安全是否得以保障。什么是信息安全？怎样才能保障信息安全？这些问题都是严肃的科学和技术问题。面对人机结合和非线性、智能化的复杂信息巨系统，我们还有许多科学技术问题需要认真研究。我们不能在研究尚处肤浅的时候，就盲目乐观地向世人宣称，我们拥有了全面的解决方案；我们也不能因为面对各种麻烦，就灰头土脸，自暴自弃，我们需要的是革命的乐观主义精神、坚忍不拔的奋勇攀登科学技术高峰的坚定信念。

人是有能力认识真理的，今天对信息安全的认识，就经历了一个从保密到保护，又发展到保障的趋近真理的发展过程。因为信息安全的问题不仅仅是因为技术原因引起的，它涉及人、社会和技术等因素，因此，仅仅靠技术是不能有效地实施信息安全保障的。从社会学的观点来看，只有依靠有信息安全觉悟和技能的人及科学有效的管理来实施综合的技术保障手段，才能取得良好的效果。

为了推动我国信息化发展的进程，信息安全国家重点实验室组织编写了《信息安全国家重点实验室信息安全丛书》。在本丛书的编写过程中，我们既注重学术水平，又注意其实用价值。本丛书从信息安全保障体系、操作系统安全、数据库安全、网络安全、无线网络安全、网络攻击、密码技术、PKI 技术、信息隐藏、安全协议、安全事件应急响应、量子密码等多个角度，分析和总结信息安全的科学问题以及信息安全保障的理论与技术，因此，这套丛书有较大的适用范围。我们将努力把国内外信息安全的最新研究成果写进书中，以使读者阅读本丛书后在理论、方法、技术上得到新的启发和收获，从而切实解决工作中的实际问题。

本丛书的组织方式是开放式的，今后将根据学科发展陆续组织出版信息安全领域的优秀图书。

信息安全只能是相对而言，它是动态发展的。任何人都不能宣称自己终极了对信息安全的认识。让我们一起努力，不断地深化自己的研究，借鉴国外先进的科学技术，结合国情，与时俱进地推出信息安全保障的新理论、新办法和新手段，用我们的智慧保卫我们的信息疆土，使我们的信息家园尽量祥和安宁。

限于作者的水平，本丛书难免存在不足之处，敬请读者批评指正。

《信息安全国家重点实验室信息安全丛书》编委会

2003 年 7 月

前　言

1969年，哥伦比亚大学的年轻学者Stephen Wiesner首次提出了采用量子物理方法保护信息的思想，鉴于当时的科技水平，他的思想被打入冷宫长达10年之久。但是，Wiesner的思想为密码学的新分支——量子密码打开了一扇小小的窗户，让后来者看到了里面的精彩。在美国IBM公司研究人员Charles H. Bennett和加拿大密码学研究人员Gilles Brassard以及后来者的推动下，量子密码最终发展成为一种颇具吸引力和应用潜力的信息保护手段，并形成了较完善的理论体系，成为密码学的一个重要分支。

以数学为基础的当前广泛使用的密码系统(本书称为数学密码)利用数学难题设计密码协议和算法，利用求解数学难题的困难性保障密码方案的安全性。与此类似，也可认为量子密码算法和协议是利用求解问题的困难性或者不可能性来保障方案的安全性。不过，这些问题是物理问题而不是数学问题，求解这些问题也必须通过物理方式实现。下面是量子密码中的两个基本问题。

问题1：如何在不损坏原来量子比特的情况下判定一个未知量子比特的精确值，或者精确区分两个或多个非正交量子比特。

问题2：如何同时精确测量量子比特中两个或多个非共轭量。

通过物理和数学方法已经证明，上述两个问题的求解是不可能的。在第一个问题的基础上产生了量子不可克隆定理；在第二个问题的基础上产生了海森堡(Heisenberg)测不准原理。显然，从基本思想方面来看，量子密码和数学密码是一致的，都可以被认为是通过求解问题的困难性来实现对信息的保护的，只是量子密码中对问题的求解是通过物理方式实现的，且上面所列的两个基本问题的求解是不可能的。

量子密码的主要特点是对外界任何扰动的可检测性和容易实现的无条件安全性，这些特征依赖于量子系统的内禀属性：测不准性和不可克隆性。对扰动可检测性的物理基础是海森堡测不准原理；而无条件安全性的物理基础是量子不可克隆定理。前者保证了任何攻击行为都可能被检测出来，后者保证了量子密码系统的安全特性。上述特征使得量子密码不但具有良好的学术价值，从而吸引了众多学科(如密码学、物理学、量子光学、计算机科学、通信和数学等)的研究人员参与该领域的研究，而且在很短的时间内受到了美国、加拿大、日本、中国以及欧盟等国家和地区的高度重视。

经过二十余年的研究与发展，量子密码不但在理论上形成了自身的框架体系，

在技术上也取得了飞速的发展。国际上许多大学和研究单位(如美国哈佛大学、波士顿大学、英国电信、瑞士日内瓦大学、日本国家信息与通信技术研究所等)纷纷成立了量子密码和量子通信方面的研究机构。除了这些研究机构外,国际上也开始出现专门从事量子密码和量子通信技术产品研发的公司,目前主要有瑞士的 id Quantique 公司、美国的 MagiQ 公司等。这些公司已经研制出了一些量子密码方面的产品,如 id Quantique 公司的量子密钥分配系统、量子随机数发生器、单光子检测器等,以及 MagiQ 公司的量子保密系统等。量子密码技术的逐渐成熟以及相关产品的问世,标志着量子密码不久将进入商用时代,并潜在着良好的应用前景。

自 20 世纪 80 年代提出量子计算机的概念以来,量子计算的机制与模型不断完善。随着量子计算机技术的迅速发展,目前广泛使用的密码系统受到了很大的威胁。分析表明,若量子计算机成功实现,以 P.W.Shor 提出的量子因式分解算法为基础,可在很短的时间内破译 RSA 算法;若以 L.K.Grover 提出的量子搜索算法为基础,可在 4 分钟内破译 DES 算法(以 10^6 次/秒的速度计算)。虽然量子计算技术目前还很不成熟,但是,按照著名的 More 定律,到 2012 年将可实现对单个原子的编码,为量子计算机的实现提供技术基础。量子计算技术的发展使得量子密码可能成为一种重要的密码体制。

本书以作者多年的研究成果为基础,结合量子密码在国内外的研究进展,经过归纳整理构建了量子密码的框架体系。为了使本书内容自成体系,书中所涉及的基础知识(如量子力学、密码学等)在相关部分作了适当的介绍。若读者已经具备这些方面的基础知识,阅读时可跳过相关章节。密码学是一门实用性很强的学科,作为密码学的分支——量子密码也不例外。考虑到这个特征,本书重点从密码学的角度阐述量子密码的概念和方案,而避开了相关物理问题的深入讨论,以免喧宾夺主。关于量子密码物理基础的深入讨论,读者可参阅国内外的有关书籍。

本书共分为 9 章。第 1 章介绍密码学和量子密码的整体发展情况;第 2 章研究量子比特的基本属性;第 3 章研究量子密钥的特征以及密钥的管理与应用;第 4 章研究量子数据加解密算法;第 5 章研究量子认证理论与技术;第 6 章研究量子秘密共享的基本理论与方案;第 7 章介绍量子密码的安全协议;第 8 章构建量子密码系统的安全性理论;第 9 章研究如何从技术上实现量子密码系统,并介绍几个典型的量子密码器件与系统。

1997 年,作者在西安电子科技大学王新梅教授的指引下有幸进入这个充满挑战的领域。两年后,西安电子科技大学王育民教授鼓励作者撰写量子密码方面的著作。经过多年的艰苦努力,终于完成此书。在此书稿完成之际,对两位教授表示衷心的感谢。另外,在本书的出版过程中得到了中国科学院信息安全国家重点实验室冯登国研究员、上海交通大学陈克非教授、科学出版社鞠丽娜女士和刘亚军女士的支持与帮助,并得到了国家自然科学基金项目(项目编号:69803008,60102001,

60472018,90104005)的资助,在此表示感谢。在本书的撰写过程中,齐源渊女士以及何广强、周南润、姚军等博士研究生校对了部分章节的文字,在此感谢他们为本书所做的工作。

期望本书能为读者起到抛砖引玉的作用,同时也期望能得到读者的批评与指正。

目　录

第1章 绪 论

随着计算技术与通信技术的飞速发展，人们对信息的需求与日俱增，人类社会正在步入信息化时代。与此同时，各种非法获取有效信息的事件不断发生，使得信息的保护越来越受到人们的关注。信息保护涉及许多方面的因素，包括自然灾害、网络或系统本身的漏洞、管理方面的缺陷、协议结构的不完善性、对信息处理的方式等。所有这些因素可以归纳为三个主要方面：人为因素、物理因素和信息的安全处理方式。为了防止这些因素造成信息的丢失和泄密，人们采取了许多安全策略，如加密、软硬件控制、各种物理控制、严格的管理制度等。但是，在信息安全与数据保护方面，即在对信息的安全处理模式方面，密码学提供了保护信息的重要方法与手段。

人们对信息安全的各种需求不断促进密码学的发展。为了获得具有高安全强度且实现简易的信息安全系统，许多学科的学者和科学家试图从不同的学科和角度研究信息安全的机制和实现手段，由此出现了从数学理论出发的基于数学的密码体制、从物理学角度出发的基于物理学的密码体制、利用生物特性设计的生物密码体制等。由于基于数学的密码体制在信息保护中的悠久历史和重要性，人们习惯于将目前所提出的密码系统划分为两大类：数学密码和非数学密码。但是，不管如何划分，所有密码体制都具有共同的特征和目标，主要区别在于这些密码体制实现的手段和密码系统的设计原理。

本章首先介绍密码学的基本概念和表现形式，以及这些密码表现形式所具有的基本特征；然后，阐述量子密码的起源、主要特征、目前的状况以及与其他学科的关系等方面的问题。

1.1 密码学的基本概念

作为一门科学，早在几千年前就有了密码学的雏形并在实践中得到应用和发展。但是，直到20世纪40年代密码学才具有系统的科学体系结构，因此，密码学是一门古老而年轻的科学。从学科发展历程来看，密码学经历了从神秘到明朗，从纯军事应用到商用，从艺术（技巧）形式到科学研究的进程。目前，密码学正得到广泛应用和普及，成为国家安全、经济活动和人们生活中的重要组成部分。从学科发展来看，经过多个不同学科的交叉与融合，以及成果的不断积累，密码学的内容得到不断的丰富和完善，成为一门典型的跨多个学科的交叉学科。

密码学是研究将可理解的符号（串）变换为不可理解的符号（串）及其逆变换的方法、手段、理论，并分析这种变换可能存在的破译方式和获取有效信息的可能性的一门科学。因此，密码学的本质就是“变换”以及对这种“变换”的分析。当然，密码学中的“变换”不是任意的，必须保证合法用户容易实现，而非法用户从经过变换后的符号序列中恢复出原来的有用信息成为不可能或者非常难，以至于破译系统将得不偿失。实现这个目标可以采用不同的机理来实现所需的变换，如数学方法、物理方法、化学方法、生物方法、电子方法、光学方法等，这也正是密码学可以跨多个学科的根本原因。在同一种方法中，还可采用不同的方式来实现所需的变换。例如，在以数学难题为基础实现的密码系统中，可以通过 DES、RSA、椭圆曲线密码体制等不同的实现手段实现对信息和合法数据的保护。

在密码学的定义中涉及几个基本概念，这些概念在密码学中作了专门的定义。下面简单介绍这些概念：表示有效信息的可理解的符号（串）称为明文，经过变换后得到的符号（串）称为密文，明文和密文的可能取值所构成的数学空间分别称为明文空间和密文空间；将明文变换为密文的过程称为加密变换，其逆过程称为解密变换，加密变换和解密变换对应的算法分别称为加密算法和解密算法；控制加密和解密变换的控制参数称为密钥，其中控制加密变换的密钥称为加密密钥，控制解密过程的密钥称为解密密钥；加密密钥和解密密钥可以相同（对称），也可以不同（非对称）；若加密密钥和解密密钥相同（对称），对应的密码系统称为对称密码系统，否则称为非对称密码系统；在经典密码学（按照学术界的惯例，本书中的经典密码是指除量子密码外的密码体制，即“经典”相对于“量子”而言）中，非对称密码系统又称为公钥密码系统。

密码学包含保密和密码分析两部分，其中保密学研究如何对信息做加密与解密处理及其相关理论；而密码分析学则研究密码系统的安全性和从密码系统中获取有效信息的方法与理论。从本质上来说，保密与密码分析是矛盾的两个方面，他们的目的正好相反，但两者又是相互关联的。通常，完善的密码分析有助于获得真正安全的密码系统。

1.2　密码学的起源与发展

密码学是一门古老而年轻的科学，经历了几千年的演化与发展后，形成了丰富的内涵，并得到了广泛的应用。根据密码学的发展历程中表现出来的特征，著者认为密码主要表现为四种形式：艺术（技巧）密码形式、古典密码形式、计算机密码形式以及非数学密码形式。密码的几种表现形式存在着关联和共性，但它们又各有其自身的特点。值得强调的是最近发展起来的基于非数学密码形式的密码系统，在这种密码形式中，目前主要有量子密码、混沌密码、光学模式识别密码等基于物理