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

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 1/21

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〈科印〉)

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

学原理的密码系统,以及基于生物学理论的生物密码体制。在非数学密码中,量子密码是目前最引人注目的密码体制。

1.2.1　艺术密码

艺术密码[1]是密码学的原始表现形式,这种形式的密码主要通过一些技巧将信息隐藏在语言文字、符号、图片等公开代码中。从某种意义上来说,这种密码形式更多的是作为一种游艺和欣赏,而不是作为实用的信息保护体制,因此这种密码形式又可称为技巧密码形式。但是,在艺术密码基础上发展起来的隐写学却是一门非常有实际意义的密码学分支,甚至有人认为隐写学已经成为一门与密码学并行的独立学科。

艺术密码可以通过多种方式实现,主要的方式有:文字变形、在艺术作品(如绘画、书法等)中加入巧妙的手笔、符号的适当排列、物理化学方法,以及哑语和手势等。在现代社会中,艺术密码仍是人们感兴趣的密码形式,常在艺术作品和文字游戏中出现。下面介绍几种实现艺术密码的方式。

第一种,通过文字变形实现的艺术密码。早在四千年前的古埃及,人们就开始学会了使用文字来隐藏信息。在尼罗河畔的梅尼特库孚镇,为了记载贵族克努姆霍特普二世所建立的功勋,某擅长书写的记述者写出了记载他领主生平的象形文字,从而揭开了有文字记载的密码史。贵族克努姆霍特普二世墓碑上的铭文,不是一种现代文明所知的密写体制,而是用一些奇怪的象形符号代替了普通象形文字,记载着他在阿梅连希第二法老王朝供职期间所建立的功勋,如图 1.2.1 所示。采用这些象形符号的意图不在于使内容难懂,而是赋予铭文以庄严和权威。因此,铭文虽不是密写的,却已具备了密码学的一个要素:文字书写的有意变形。随着埃及文化的兴盛,书写文字得到了不断发展,这些变形逐渐变得更复杂、更巧妙、更普遍,伴之而来的是许多铭文第一次具备了密码学的第二要素:秘密性。在少数情况下,秘密性是为了增加宗教著作的神秘力量,但是,在更多的情况下秘密性是出自埃及人要过路行人和后人读他们的墓志铭,从而向死者祝福的愿望。这种通过文字变换来隐

图 1.2.1　象形文字的碑文:特殊形式(左)和普通象形文字(右)

藏信息的方式显然已经包含了密码学中的秘密性和变形（即明文→密文）两大要素，因此它属于密码学的范畴。

在接下来几千年的发展中，这种简单的文字变换被人们视为一种艺术，因为人们关心的是这种变换所表现的形式而不是目的。由于这种变换的趣味性以及这种方式能体现设计者的智慧，文字变形得到了不断的发展。图 1.2.2 所示是一种典型的通过文字变形来实现信息隐藏的密码形式。在文字变形的基础上还产生了一些新的利用语言文字隐藏信息的方法，如利用句子或段落的特点、句子的首字等隐藏信息。受这种方式的启发，在经典密码中发展了阈下信道理论。

图 1.2.2　Charlemagne 的秘密字符

第二种，通过艺术作品中的某种方式或某些手笔隐藏信息。不但可以通过文字变形或变换来隐藏信息，实现密码形式，一些绘画与艺术作品也常被人们加以利用来隐藏信息。例如，利用人体大脑的双稳特征，即人的视觉暂留特征，一副艺术作品中可以包含两种不同的信息，如图 1.2.3 所示，图示包含了“奖杯”和“人头”两种不同的信息。图 1.2.4 是一幅带密码的风景画，其中包含了一段隐藏的信息，画中沿河岸的短草叶代表莫尔斯电码的点，长草叶代表莫尔斯电码的划，拼出的文字为：“*Compliments of CPSA MA to our chief Col Harold R. Shaw on his visit to San Antonio May* 11^{th} 1945.”

图 1.2.3　包含两种不同信息的艺术图

图 1.2.4　一幅带有密码的风景画

第三种，通过符号的适当排列隐藏信息。在选定某几个符号所构成的符号序列中，符号序列表面上表示一种公开的意义，但是，符号序列的排列中却隐藏了另外

一种信息。图 1.2.5 所示是通过跳舞人符号的排列来隐藏信息的。

图 1.2.5　通过跳舞人符号隐藏信息

除了上述方式外,日常生活中我们还遇到过其他许多隐藏信息的艺术密码形式,如肢体语言、白纸显字等。

总之,艺术密码所要完成的任务就是将易懂的交流信息,通过一些变形或变换使其变成难以理解的信息。艺术密码虽然是在古代产生的,但在现代生活中仍然存在。值得指出的是,在艺术密码与现代信息科学相结合的基础上发展起来的隐写学,已经成为信息保护中的重要分支,隐写学在当今的信息保护,如数字产品的版权保护、合法性、安全性等方面可能发挥重要的作用。

1.2.2　古典密码

密码学与其他学科一样,随着社会的需求而产生,并随着社会的进步而发展。经过上千年的演化与发展,由于政治、军事和外交等领域的需要,安全性成为密码的关键因素,原始的艺术密码不能保证这种安全,于是,密码学逐渐从艺术形式中摆脱出来,形成了密码学的古典密码形式[2]。古典密码的特点是“替换”,替换是一种线性变换,因此古典密码本质上是一种以线性代数为基础的密码形式。正是这个原因,在后来的发展中密码学越来越与数学密不可分,数学成为密码学的重要基础。当然,数学不是密码学的唯一基础,后面将会了解到密码学可以与许多学科发生紧密联系。古典密码在近代,特别是在两次世界大战期间得到了空前的发展,在这一时期人们提出了许多优秀的古典密码体制。虽然有些密码体制现在很容易被破译,但是,它们对现代密码体制的设计仍有重要的参考价值。古典密码体制中常见的密码体制有恺撒密码、Vernam 密码等。关于这些密码体制的详细介绍可参看文献[1]。

古典密码系统可以用手工、机器、电子等手段来实现。通过手工的方法实现的密码比较简单和直观,但其安全性差。机器密码是两次世界大战的产物,用转轮密码机来实现,它在两次世界大战中都曾被广泛使用。相对于手工密码,机器密码具有较好的安全性能。法国、日本、德国等国家的军队都曾使用过转轮密码机。图 1.2.6所示是一台德国的转轮密码机,由 Arthur Scherbius 于 1919 年发明。而电报、无线电的发明使古典密码学获得了飞速的发展,图 1.2.7 所示是一台英国的在线密码电传机,由 Lorenz A.G 大约在 1943 年制造。

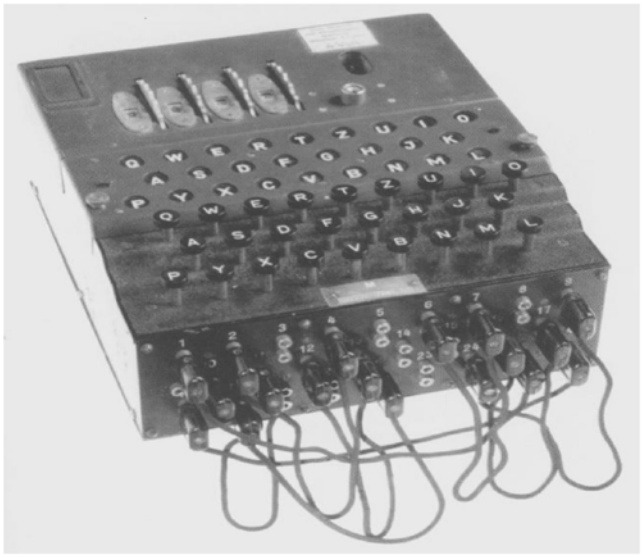

图 1.2.6　转轮密码机 ENIGMA

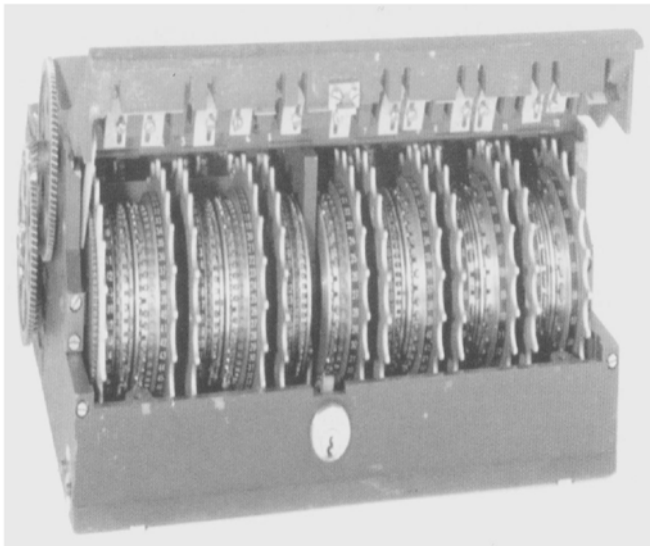

图 1.2.7　在线密码电传机 Lorenz SZ 42

由于军事上的需要,古典密码分析学也得到了迅速发展。密码和密码分析不但在信息保护中起着重要的作用,在某种意义上甚至可能改变社会的发展进程。例如,第一次世界大战的第一天,英国海军训练局的艾尔佛雷得· 尤图爵士着手创办了一个后来几乎成为传奇式的,并对历史进程产生直接而显著影响的密码分析部门。该部门的密码分析人员威廉· 蒙哥马里和他的一位年轻同事奈杰尔· 德格雷于 1917 年 1 月 17 日上午 10 时半许破译了一份德国人的密报,该密报谈到了德国可能与美国交战,英国有关部门通过十分巧妙的方式通知了美国有关方面,使得居住在北美洲中部不受欧战遥远枪炮声刺激的美国人,猛然发现战争离他们并不遥远。曾在三个月前说过把这个国家引入战争就是“对文明犯罪”的威尔逊,这时断定“公道比和平更宝贵”。这一份密码的破译结果导致美国参战。另外,在第二次世界大战的中途岛战役中,由于美军成功地破译了日军的密码,成功击落了山本五十六的座机,从而取得了决定性的胜利。有关专家认为,由于同盟军在密码战役上的胜利,使第二次世界大战至少缩短了八年。这些足以说明密码学在历史上的重要地位。

但是,由于密码学在军事领域的特殊地位,古典密码的研究被罩上了一层神秘的面纱,其研究基本上是在一种封闭的状态下进行的,这种状况在某种程度上阻碍了密码学的进展。

1.2.3　计算机密码

1949 年,美国贝尔实验室的科学家 C. E. Shannon 发表了他的论文《保密系统的数学理论》,文中以严格的数学理论为基础,系统地研究了密码系统及其相关问题,从而为密码学提供了科学依据。在这篇论文中,Shannon 提出了完善保密性、实

际保密性等概念,从数学意义上建立了密码学,特别是对称密码的基础理论,并用该理论首次证明了 Vernam 算法(一次便笺)的完善保密性问题。Shannon 保密通信理论的建立,使密码学第一次有了科学的理论依据,为密码学的系统研究打下了基础,同时使密码学成为系统化的科学,成为真正意义上的学科。

随着电子技术的发展和计算机技术的成熟,密码学获得了飞速的发展。计算机的诞生对古典密码产生了很大冲击,许多当时由于破译时计算复杂而难以破译的密码算法在计算机面前显得不堪一击。同时,计算机的广泛应用和网络技术的发展使得密码学不再是军事领域的"自留地"。计算机科学的进步大大促进了密码学的变革,正如德国学者 T. Beth 所说:"突然,现代密码学从半军事性的角落里解脱出来,一跃成为通信科学领域的中心研究课题"。可以说,计算机促进了密码学的进一步发展,加上以 Shannon 理论建立起来的密码系统非常适合工程上的实现,由此产生了可在计算机和电脑芯片上运行的密码形式——计算机密码[2,3]。

所谓计算机密码是指建立在 Shannon 保密通信理论基础和计算复杂性基础上的以计算机或计算机网络的计算能力来保证其安全性的密码系统。图 1.2.8 所示是一块用于独立式或网络计算机的密码板,由瑞士 Crypto AG, Zug 于 1996 年制造。计算机密码的特点是以计算复杂性来保证密码系统的安全性。由于计算机的普及,计算机密码在政治、军事、外交、经济等领域以及日常生活等各个方面都发挥着重要的作用。

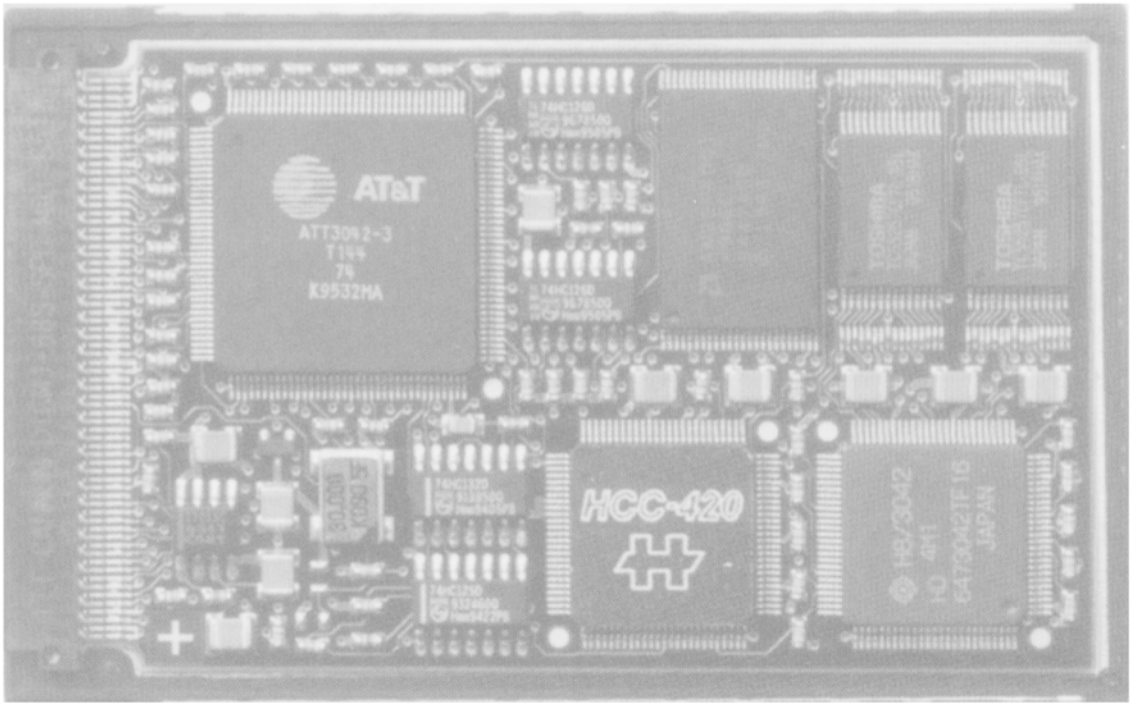

图 1.2.8　用于独立式或网络计算机的密码板

对称密码体制是计算机密码中的一种重要的密码体制,这种密码体制的基本思想是加密密钥和解密密钥相同或者对称。因此,这种密码体制要求所有密钥都被

严格保密,不得有任何泄漏。对称密码体制包括序列密码和分组密码。序列密码主要用于军事、外交等领域,其安全性由计算复杂性理论保证。从某种意义上来说,可以认为二进制体系下的序列密码是 Vernam 算法的简化形式,这种简化虽然降低了密码系统的安全性,却增强了系统的可操作性。分组密码中典型的密码系统是 DES。从 20 世纪 70 年代开始,计算机的应用在发达国家得到了迅速的推广,计算机被广泛应用于商业、通信等民用领域,旧的密码体制不堪一击,各种计算机犯罪不断上升,各公司为了维护自己的切身利益,不断增加系统的安全投资,并纷纷研究各自开发的密码系统。由于形势的需要,美国国家标准技术局(NIST)于 1973 年开始征集用于商业的数据加密标准,后来选中了 IBM 公司的一个算法——LUCIFER 算法,1977 年 7 月 15 日正式生效为美国商用数据加密标准(简称 DES)。由于计算机网络的飞速发展,经过二十多年的使用,DES 完成了它的使命,最终在穷举密钥攻击下被破译(因为 DES 的密钥空间只有 2^{56})。为了寻找 DES 的替代者,NIST 再次征集新的数据加密标准,历时 5 年,于 2001 年 11 月 26 日正式公布了新的数据加密标准 AES (Advanced Encryption Standard)。分组密码的一个主要特点是加密速度很快,便于在计算机芯片上实现,但在身份认证和数字签名中缺乏优势。

非对称密码体制是计算机密码中的另一种重要密码体制,基本思想是加密密钥和解密密钥不对称。也就是说,由一个密钥可以容易地导出另一个密钥,但是逆过程很难实现。因此,非对称密码体制本质上是一个单向函数。单向函数有两种形式:严格单向函数和陷门单向函数。所谓严格单向函数就是具有不可逆性的单向函数,这种函数没有对应的反演函数。例如,时间的流逝、生物的成长过程等都可用严格单向函数描述。严格单向函数的特点是任何人采用任何方法都不能获得其逆过程。因此,严格单向函数不能用于加密和解密,但可用于身份认证和签名。陷门单向函数是在知道某种条件的情况下可获得其逆过程所对应的函数,这里的条件称为陷门。显然,只要知道陷门就可以获得与单向函数对应的反演函数。因此,陷门单向函数被广泛应用于非对称密码体制。需要指出的是,在计算机密码中所使用的陷门单向函数都是基于计算复杂度的,对应的安全性属于计算安全。由于非对称密码体制采用陷门单向函数,密码算法中部分密钥可以像电话号码一样公开,因此,非对称密码体制也称为公钥密码体制。非对称密码思想是 1976 年 Whitefield Diffie 和 Martin E. Hellman 首先提出来的,这种思想使密码学的思维方式发生了变革。不久,著名的 RSA 算法即告诞生。在此基础上,一些重要的公钥密码算法如 Rabin 密码算法、McEliece 密码算法、椭圆曲线密码算法等相继被提出。

计算机密码的第三个重要方面是在认证中的应用。随着网络和通信技术的飞速发展,网上的各种活动越来越多,这些活动导致了对身份认证、数字签名和消息确认等方面的强烈需求。计算机密码,特别是计算机密码中的公钥密码体制在这个

方面具有良好的优势。目前,认证已成为计算机密码中的重要组成部分。

计算机密码取得了很大的成功,并将继续在信息保护方面发挥重要作用,但也存在一些问题。首先,计算机密码不能提供具有无条件安全的密码方案。虽然Shannon证明了 Vernam 算法的无条件安全性,由于在证明过程中假设一个安全信道的存在,使得 Vernam 算法存在所谓的 Catch 22 问题。同时,在密钥管理方面也存在很大的困难,这些问题使得 Vernam 算法的"无条件安全性"在应用中难以得到根本意义上的保证。其次,计算机密码的安全基础——计算复杂性也给计算机密码带来了一些缺陷。一方面,基于计算复杂性的密码系统不能提供无条件安全的密码方案,使得用户在购买或实际应用时有一定程度的担心;另一方面,计算复杂性依赖于计算技术、网络和通信技术的进步,这些技术的进步将导致相应密码系统的安全性受到威胁。最后,量子计算机的迅速发展威胁计算机密码的安全性。量子计算机以量子并行计算原理为基础,使得计算速度远大于电子计算机。一旦量子计算机研制成功,计算机密码中的大部分算法将受到巨大的威胁。研究表明,用量子计算机破解 RSA 算法和 DES 算法只要几分钟量级的时间 (见第 8 章)。当然,"矛"与"盾"总是同时存在的,我们有理由相信,随着量子计算机的出现,必有针对这种计算能力的计算机密码系统。事实上,目前已经有学者在探索基于量子计算复杂度的公钥密码算法 (见第 4 章)。

安全性高而易于实现的密码系统是密码学的追逐目标之一,为了解决密码学中存在的问题,并促进密码学的发展,不同学科的学者和科学家积极探索实现信息保护的新机制和新方法。到目前为止,人们已经提出了许多新型密码体制,如基于物理学的密码体制、基于生物学的密码体制等。下面对基于物理学的密码体制作简单介绍。

1.2.4　物理密码

所谓物理密码是指以承载信息的载体 (即各种物理信号,如电信号、光信号、量子信号等) 和相应的物理系统的内禀物理属性对信息进行密码处理,从而实现信息保护的方法、手段和理论。在这种密码系统中,信息载体 (如信号) 和物理系统 (如信道) 之间相互作用,因而他们之间相互影响。显然,这种方式与计算机密码方式完全不同,在那里,信息载体和物理系统间的影响可以忽略,从而可以采用通用的数学理论——Shannon 信息论来描述,采用比特"0"和"1"及一些算法和协议即可有效地描述,而不必关注具体的通信系统。但在物理密码中,由于信息载体和物理系统之间的相互影响突出,不同的物理系统对应不同的处理方式。已经提出的物理密码有量子密码、混沌密码、光学密码等三种形式,其中,应用前景最明朗的是量子密码和混沌密码。

量子密码是 1969 年提出来的[5],它利用微观粒子的量子属性实现对信息的保

护。一个最基本的量子属性是测不准原理,这是量子物理学的一个基本原理,该原理表明两个具有互补性的物理量不能同时精确测量。例如,对于一个粒子的位置和速度,如果该粒子是一个宏观粒子(如钢球),按照牛顿力学理论,在任何时刻该粒子的位置和速度都可同时被精确获得。可是,对于微观粒子,量子力学理论表明对该粒子的位置和速度不能同时精确测量。也就是说,若精确获得该微观粒子的速度,则其位置完全不能确定,反之亦然。测不准原理的一个重要推论是未知量子态的不可克隆定理。量子不可克隆性与经典物理学规律和日常生活中的现象明显不同。人们常常谈论"克隆植物"、"克隆羊",可是,"克隆"现象在微观世界中并不总是存在,量子态的不可克隆性遵循量子不可克隆定理。不可克隆定理和测不准原理为量子密码提供了安全性保障,使得量子密码方案可以具有无条件安全性,且可通过物理方式实现。自 20 世纪 80 年代起人们对量子密码学给予了足够的重视,获得了大量的研究成果[6~10],目前正受到科学界和政府、军事部门的高度关注。到目前为止,在量子密码方面已经成功地研制出了一些实用化产品,图 1.2.9 所示是瑞士 id Quantique 公司 2001 年研制的量子密钥分配系统。该系统可在光纤中 60 km 的范围内实现量子密钥分配,传输速率为 1 kb/s 左右。据最新报道,目前可在超过 100 km 的光纤中实现量子密钥分配。通过互联网搜索,容易发现量子密码技术与应用日新月异。

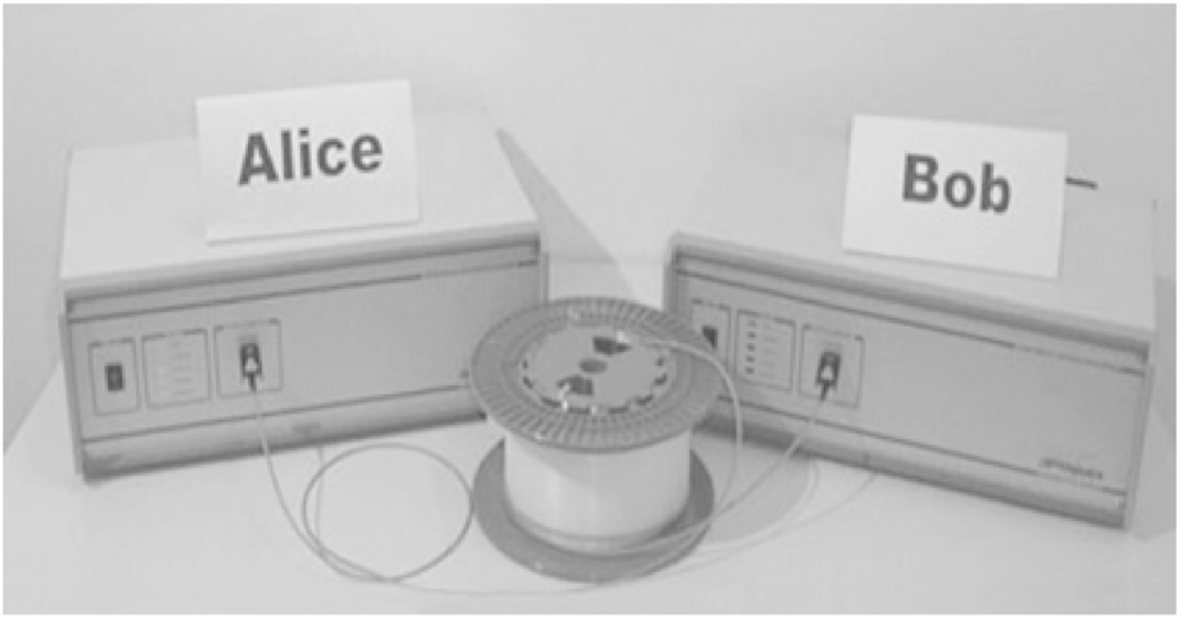

图 1.2.9　id Quantique 公司研制的即插即用量子密钥分配系统

混沌密码是另一种形式的物理密码[11~16],是一种利用混沌现象实现信息保护的密码系统,其物理基础是混沌动力学。对混沌现象的研究始于 20 世纪 70 年代。所谓混沌是指由确定性动力学系统产生的一种看似随机的非线性现象。混沌信号具有的非周期性、连续宽带频谱、类似噪声的特性使它具有天然的隐蔽性,对初始

条件和微小扰动的高度敏感性,又使混沌信号具有长期不可预测性。混沌现象作为一种特殊而复杂的非线性运动行为,在物理学、信息学、气象学、生物学、电子学和经济学等领域得到了广泛的研究和应用。在密码与保密通信方面,混沌信号的特点非常适合构造基于混沌特征的密码系统。但是,混沌信号对扰动高度敏感的特点也为实际系统中如何控制混沌系统并使之为人们所用带来了困难。为了实现控制混沌的目的,1983 年 Tang 等在 IEEE 的《电路与系统》杂志上建议了一种用混沌电路对输入信号实现同步控制的思想。此后 Pecora 和 Carroll 对混沌同步做了较深入的研究,提出了混沌同步理论,并用相关电路实现了同步。1990 年,美国学者 E. Ott 等人又提出了混沌控制的原理。至此,人们发现混沌现象虽然是不确定的、对初值敏感的,但可以采取有效的方法去控制进而利用混沌信号为人们所用,由此,混沌密码引发了人们普遍的兴趣。

近十多年来,混沌保密通信得到了快速的发展,利用各种混沌系统实现了模拟和数字信号的保密通信实验研究。混沌保密通信的基本原理是利用混沌信号对信息加密,然后在解密端采用同步技术实现信息的解密。加密方法有四种:混沌遮掩(chaotic masking)、混沌调制(chaotic modulation)、混沌键控(chaotic shift keying)和混沌扩频(chaotic spread spectrum)。这些技术构成了混沌保密通信的核心技术,确保了混沌系统的成功实现。

混沌系统的计算机化是混沌密码中的另一个研究方向,这种方法采用计算机技术或数字电子器件仿真混沌系统,并由此产生混沌序列。这些混沌序列被用于设计序列密码和分组密码,甚至被用来设计公钥密码系统。但是,由于这种条件下生成的混沌序列都是在计算机或其他有限精度的器件上实现的,特别是经过取模(像经典密码中的“mod N”)处理,所生成的混沌序列将出现特性的退化,主要表现为周期缩短、相关性加强以及线性复杂度降低等特征。这些特性导致混沌序列的无限相空间特征退化为有限相空间,从而降低了密码系统的安全性。因此,混沌序列的特性退化问题成为这个方向的重要研究课题。

实际应用中,混沌保密通信可以通过电子、光学、物理等方法实现,混沌密码和混沌保密通信正在逐步实用化。混沌同步是混沌密码和混沌保密通信在技术上的主要困难,一旦找到有效、廉价的混沌同步系统,混沌密码将可能在计算机网络、光纤网络、卫星等通信系统中得到应用。

最后一种物理密码是基于信息光学的光学密码体制,这是 Javidi 等人于 20 世纪 90 年代初提出的一种新型物理密码[17~20]。这种密码系统利用光学模式识别,特别是光学图像处理中的傅里叶变换实现对信息的加密。基于光学信息处理的加密方式可在两方面得到应用:①用于通信网的加密系统,在这方面的应用中采用二次相位屏蔽编码技术加密,将加密数据加载到光信号或电信号中发送出去,在接收端再采用相位技术接收;②用于身份验证,如个人身份卡等,可用一次相位编码技术,

将个人身份等信息存储在个人身份卡中,再将个人身份存放在验证身份的机器中,采用光学神经网络算法进行个人身份验证。基于光学模式识别的保密系统中所用器件为光学元件,如透镜、相干光源等,不需要对数据进行复杂的算法和大量的二进制数据处理。与电子元件组成的方法相比,这种方法具有一些优点,如传输信息大,速度快等。但是,这种物理密码没有受到人们的重视。

1.2.5 几种密码形式的比较

为便于比较和理解,下面将密码学的四种表现形式从实现原理、加解密方式、安全性、实用性等方面作一个简单的比较(见表 1.2.1)。

表 1.2.1 四种密码形式的比较

	艺术密码	古典密码	计算机密码	物理密码
实现原理	艺术变形	简单代数	数学理论	物理规律
密钥	简单编码规则	数学参数	数学参数	物理参数
信息处理方式	艺术变形	代数运算	复杂算法	物理操作
安全性	差	差	较好	好
实用性	欣赏	密码基础	好	一般
性价比	差	差	好	一般

从表 1.2.1 来看,计算机密码仍然是目前最适合应用的密码系统,但由于其计算安全性而存在一个先天的缺陷,这正是许多安全系统经常遭受攻击的主要原因之一。显然,在安全性方面物理密码是最强的密码体制,但由于目前物理密码处在实验研究或实用化研究阶段初期,除了在军事、政府等机要部门外,物理密码目前还不很适合商用。但可以相信,技术的进步会使物理密码具有优良的性价比,从而为物理密码的应用开辟一个新的天地。因此,物理密码具有良好的应用前景。

鉴于物理密码的高安全性和计算机密码的强实用性,两者的结合成为一个新的方向。在此基础上可将量子密码技术应用于当前的实际系统中。实际上,国际上正在开发的基于网络的密钥分配系统就是采用这种融合技术实现的。

1.3 量子密码的起源与发展动态

1.3.1 量子密码的起源

利用量子效应保护信息是 1969 年哥伦比亚大学的年轻学者 S.Wiesner 首先提出的。当时,Wiesner 写了一篇题为《共轭编码》(Conjugate Coding)的论文,该文提出了两个全新的概念:量子钞票(quantum bank notes)和复用信道(multiplexing channel)。量子钞票利用量子比特存储金额,类似于电子钞票。实现量子钞票的方法是利用量子比特的不可克隆性来储存一定数量的金额。由于量子

比特的不可克隆性,量子钞票具有无条件安全性。从目前的情况来看,理论研究表明量子比特的存储时间可为无限长,实验上也可达到分钟量级的存储时间。但是,在 Wiesner 刚提出量子钞票的时候,通过光子技术实现的量子比特的储存时间极短 (少于 10^{-8}s),按当时的技术实现量子钞票简直就是天方夜谭,因此,基于量子效应保护信息的观点没能被人们接受。另一个概念是复用信道,其实现方式是利用单量子比特实现两个经典比特信息传输,它与 1979 年 Rabin 提出的不经意传输 (oblivious transfer) 极其相似。与量子钞票不同的是,复用信道利用量子比特的传输而不是量子比特的存储来实现。研究表明,复用信道在以通用测量 (general measurement) 为基础的攻击策略下是不安全的,但攻击方案中需要用到在未来才能实现的量子计算机。Wiesner 的这篇论文开创了量子密码的先河,在密码学史上具有划时代的意义,遗憾的是这篇论文当时没能获准发表,直到 1983 年才得以面世,使得量子密码学的出现推迟了 10 年。

1979 年,Wiesner 在与他的朋友——IBM 公司的研究人员 C. H. Bennett 的一次偶然的谈话中提及他十年前的思想,引起 Bennett 的注意。于 1979 年在 Puerto Rico举行的第 20 次 IEEE 计算机科学基础会议上,Bennett 与加拿大 Montreal 大学的密码学研究人员 G. Brassard 讨论了 Wiesner 的思想,并发表了类似于 Wiesner思想的一篇论文。虽然论文中的成果很粗糙,甚至是不安全的,但毕竟重新开始了量子密码的研究。值得注意的是,最初 Bennett 和 Brassard 没能正确理解 Wiesner的思想,在 1982 年的美洲密码学会议上发表的论文中,他们利用量子比特的储存来实现量子密码并提出公钥算法,而量子比特的储存在当时的技术上仍然是不可能实现的,因此没有引起人们的共识。不久,他们意识到在量子密码中量子比特的传输比量子比特的储存更重要。基于这个出发点,1984 年 Bennett 和 Brassard 提出了著名的量子密钥分配的概念,这个概念的提出标志着量子密码的真正开始。同年,Brassard 又提出了量子掷币协议 (quantum coin flipping protocol),后来发展成量子比特承诺 (这些方案在 1997 年被证明不安全,见第 7 章)。从此,量子密码引起了国际物理学界和密码学界的高度重视,开始对量子密码的几个方面,特别是量子密钥分配方面展开了丰富多彩的研究,取得了大量的研究成果。

从 2000 年开始,量子密码开始引起商家的重视,国际上相继成立了一些量子信息处理方面的公司,具有代表性的有美国的 MagiQ 公司、瑞士的 id Quantique 公司等。到目前为止,在技术研究与系统开发方面显现出了可喜的势头,部分技术已经产品化。人们预言,量子密码将在不久的将来走向商业领域,并成为信息安全技术领域中的主要成员之一。

1.3.2 量子密码的基本特征

量子密码之所以能够被人们接纳,并成为受到密码学界、物理学界、商家、媒体、政府部门等各方面广为关注的密码学分支与技术,主要原因在于量子密码本身的特征。研究表明,量子密码具有两个基本特征:无条件安全性和对窃听的可检测性。所谓密码系统的无条件安全是指在攻击者具有无限计算资源的条件下仍不可能破译该密码系统。无条件安全又称为信息安全,其基础是信息理论,自然地,量子密码的信息安全基础是量子信息理论,但是,量子信息论还很不完善。所谓对窃听者或其他各种扰动的可检测性是指通信中的两个用户之间的信道受到干扰时,通信者根据测不准原理可以同步检测出这种干扰的存在与否。对扰动和窃听者行为的可检测性没有经典对应,是一种独特的量子效应,这种特性是保证量子密码具有无条件安全性的重要基础之一。前面提到的关于量子密码的两个基本特征是经典密码学中无法实现或难以实现的,然而,他们在量子密码中很容易实现。这些特征使得量子密码在信息保护和保密通信方面具有良好的优势,并得以成为密码学中的一个重要分支。

在目前所有已经提出的量子密码系统中,方案的实现都利用了量子信号(量子比特)的传输特性,因此,一个量子密码系统实际上是一个量子通信系统,该系统包含量子信源、信道和信宿等通信模型的基本要素。在量子信号的传输过程中,所传输的量子比特一般来自于一个非正交量子比特集合,即量子密码系统的量子信源是由非正交的量子符号集所构成。这种非正交特性保证了量子信道中传输的量子比特的不可克隆性。因此,对于任何不合法的通信用户,均不可能逃避不可克隆定理而获取有效的量子信息。另一方面,要获得有效信息,攻击者必须对量子信道中传输的量子比特做相应的物理处理(操作或测量)。由于攻击者事先并不知道量子信号处于何种状态,不可能 100% 地选取正确的测量仪器对量子信道中的量子比特进行准确测量,是一种完全随机的测量方式。这种随机测量必然会改变量子比特原来的状态,所引起的状态改变对合法通信者来说是可知的,根据状态改变的程度,合法通信者可以估计并检测出攻击者或者扰动是否存在,以此为依据判断是否进行下一步的操作。因此,在量子密码系统的无条件安全特性方面,可以认为不可克隆定理是保证量子密码无条件安全性的内禀条件,而测不准原理则是外部保障。需要指出的是,并非所有的量子密码系统都需要不可克隆定理和测不准原理同时作为其安全特性的内外保证条件。例如,在量子数据加密算法、量子多方安全协议等量子密码系统中,一般只需要不可克隆定理即可。因此,从整个量子密码学的角度来看,保障无条件安全性的基石是不可克隆定理。

量子密码与数学密码的本质区别在于它们所依赖的基础不同。数学密码以数学理论为基础,密码系统依据一个或多个数学问题而设计,其安全性由求解数学问

题的复杂性和困难性得以保证。由于数学问题均是对一类现象的抽象和高度概括，从技术实现的角度来看，一个数学密码系统可以脱离具体的实现系统而设计，设计完成后可采用多种方式实现。例如，基于大整数因子分解问题的 RSA 算法，算法的设计思想与任何具体的实现系统无关，RSA 算法的技术实现可以采用电路方式、光学方式、电磁场方式、计算机软件甚至量子方式实现对数据的加密和解密处理。量子密码以量子物理为基础，密码系统依据一个或多个量子物理规律而设计，其安全性由量子不可克隆定理和测不准原理得以保障。与数学密码不同的是，量子密码方案一般是针对一个具体的物理系统而设计的。显然，量子密码系统的适用性没有数学密码那样宽。特别是量子密码系统不能脱离实际的系统而存在。例如，针对量子比特的纠缠特性而设计的密码系统，只能采用纠缠量子比特来实现，如 EPR 协议（见第 3 章）；同样，针对量子比特的互补特性设计的量子密码系统，只能采用共轭量子比特来实现，如 BB84 协议（见第 3 章）。

量子密码起初的主要目标是为了解决经典 Vernam 算法中的密钥管理问题，因此，量子密码的研究主要集中在量子密钥的分配方面。即使经过了三十余年的研究，仍然有一些研究者将量子密码术与量子密钥分配画等号。但是，量子密码在其他方面，如量子数据加密、量子认证、量子安全多方协议、量子保密通信等方面也得到了迅速的发展，形成了系统的理论体系，有些方面还逐渐研制出了产品。可见，量子密码已经发展成为密码学的一个重要分支，而不仅仅是一项密码术。作为一个密码学分支，量子密码的目标与密码学一样，都是为了保护信息，为信息安全提供保密性、认证性和完整性方面的方法与技术以及基本理论。

1.3.3　量子密码的发展动态

量子密码是与计算机密码几乎同时代提出和发展的密码学分支，但是，三十多年来计算机密码得到了飞速发展，并成为信息保护的重要手段。相对而言，由于技术上的限制，量子密码发展较为缓慢，特别在 20 世纪 60~ 80 年代之间，几乎没有实质性进展。随着科学与技术的进步，90 年代以后，量子密码受到了人们的高度重视，取得了迅速的进展。

经过三十余年的研究，逐渐形成了系统的量子密码理论体系，内容涉及量子密钥管理、量子加密、量子认证、量子密码安全多方协议、量子密码信息理论、量子密码分析等方面。量子密码在技术实现方面，在与量子密码单元器件和量子密码系统有关的技术上都已经获得了初步的成果，一些重要的量子密码系统（如美国正在构建的基于互联网的量子密码网络系统）正在建设中，并取得了阶段性成果。

由于量子密码理论和技术日新月异，本节主要介绍量子密码的整体发展状况。

1. 量子密钥管理

量子密钥管理包括量子密钥产生、分配、存储和验证等几个部分,其中在理论和技术方面最成熟的是量子密钥分配。所谓量子密钥分配是指两个或多个合法通信者在公开量子信道上利用量子效应或原理获得秘密信息(量子密钥)的过程。1984 年,Bennett 和 Brassard 以单量子比特为基础,利用共轭量子比特的特性提出了第一个量子密钥分配协议(即 BB84 协议),该协议形式简洁,物理实现简单,然而方案具有无条件安全性。1989 年,Bennett 和 Brassard 领导的研究组从实验上首次成功验证了 BB84 协议,虽然量子比特的传输距离只有 32 cm,但该实验具有重要的意义。在 BB84 协议的基础上,英国牛津大学的年轻学者 A.K.Ekert 另辟蹊径,利用纠缠比特及其关联特性设计了 EPR 协议。从此,量子密钥分配引起了人们普遍的关注,人们从量子密钥分配的方案设计、安全性分析、实现技术等几个方面开展了全面的研究。

在方案设计方面,以 BB84 协议和 EPR 协议为基础,提出了许多改进的方案,典型的方案有 Bennett 的 B92 协议,Vaidman 等人提出的基于量子比特正交特性的方案,德国 Hannover 大学的六态协议等。这些量子密钥分配方案都是针对两方通信而设计的,当涉及三方或更多方的通信时,需要实现网络中的量子密钥分配,这个方面的代表性工作有英国电信实验室的 P.D.Townsend 等人的工作和以色列 E.Biham 等人的工作。不管是点对点还是网络中的量子密钥分配方案,均包括随机量子比特串的产生与分配、干扰检测、保密加强等过程。量子比特串的产生与分配在不同方案中的实现过程和原理不同。例如,BB84 协议中传输的量子比特是具有共轭特性的量子比特,而 EPR 协议中传输的是纠缠量子比特。通信各方获取了随机量子比特后,接下来的任务是检测系统中噪声的影响和窃听者的干扰等情况,对干扰的检测能力是经典密码中没有的,这正是量子密钥区别于经典密钥之所在,也是量子密码的优势之一。仅有前面两个过程是不够的,因为它们不能保证方案的安全性。为了获得具有无条件安全性的方案,需要一些附加的过程,通常的做法是增加一些经典处理技术,如数据纠错、保密加强技术。保密加强技术包括经典保密加强和量子保密加强,它是量子保密通信中的必要步骤,也是提高密钥安全强度的重要手段。目前,保密加强技术主要用于量子密钥分配,不过,著者认为量子保密加强技术在量子身份认证、量子签名等方面有着潜在的应用,还有待进一步研究。

在安全性分析方面,人们利用物理方法、经典密码方法针对所提出的协议分析了量子密钥分配方案的安全性。物理攻击方式主要有个体攻击、集体攻击和联合攻击三种模式。所谓个体攻击是指攻击者对信道中传输的单个量子比特进行克隆、截取、测量等处理方式来获取有效信息;集体攻击是指利用纠缠的方法将试探量子比