信息科学技术学术著作丛书

量子密码协议的设计和分析

杨宇光 著

科学出版社

信息科学技术学术著作丛书

量子密码协议的设计和分析

杨宇光 著

科学出版社
北京

内 容 简 介

本书以作者及其课题组近五年的研究成果为主体，结合国内外学者在量子密码学领域的代表性成果，对这一领域的主要内容作了系统论述，并提出了一些新的研究课题及进展。全书分为 9 章。第 1 章为绪论，主要介绍密码学的发展历史、量子密码学的发展历史、量子密码学与量子计算的关系以及量子密码学面临的挑战和应用前景；第 2 章为量子密码研究所需的量子力学基础知识；第 3～9 章分别介绍了量子密码协议的设计和安全性分析方法，主要包括量子密钥分发和身份认证、量子安全直接通信、量子秘密共享、量子签名、安全多方量子计算、量子密码协议的安全性分析方法以及量子密集编码。

本书既可作为对量子密码学感兴趣的读者的入门教材，也可作为量子密码学领域研究工作者的参考用书，适合于密码学、信息安全、信息与通信系统、信号与信息处理、物理学、数学及相关学科的高年级本科生、研究生、教师和科研人员阅读参考。

图书在版编目(CIP)数据

量子密码协议的设计和分析/杨宇光 著. —北京：科学出版社，2013
(信息科学技术学术著作丛书)

ISBN 978-7-03-037367-0

Ⅰ. 量… Ⅱ. 杨… Ⅲ. 量子-密码-通信协议-研究 Ⅳ. TN918.2

中国版本图书馆 CIP 数据核字(2013)第 084271 号

责任编辑：魏英杰 杨向萍 韩 默/ 责任校对：胡小洁
责任印制：张 倩 / 封面设计：陈 敬

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
源海印刷有限责任公司 印刷
科学出版社发行 各地新华书店经销

*

2013 年 4 月第 一 版 开本：B5(720×1000)
2013 年 4 月第一次印刷 印张：14 3/4
字数：276 000

定价：60.00 元

(如有印装质量问题，我社负责调换)

《信息科学技术学术著作丛书》序

21世纪是信息科学技术发生深刻变革的时代，一场以网络科学、高性能计算和仿真、智能科学、计算思维为特征的信息科学革命正在兴起。信息科学技术正在逐步融入各个应用领域并与生物、纳米、认知等交织在一起，悄然改变着我们的生活方式。信息科学技术已经成为人类社会进步过程中发展最快、交叉渗透性最强、应用面最广的关键技术。

如何进一步推动我国信息科学技术的研究与发展；如何将信息技术发展的新理论、新方法与研究成果转化为社会发展的新动力；如何抓住信息技术深刻发展变革的机遇，提升我国自主创新和可持续发展的能力？这些问题的解答都离不开我国科技工作者和工程技术人员的求索和艰辛付出。为这些科技工作者和工程技术人员提供一个良好的出版环境和平台，将这些科技成就迅速转化为智力成果，将对我国信息科学技术的发展起到重要的推动作用。

《信息科学技术学术著作丛书》是科学出版社在广泛征求专家意见的基础上，经过长期考察、反复论证之后组织出版的。这套丛书旨在传播网络科学和未来网络技术，微电子、光电子和量子信息技术、超级计算机、软件和信息存储技术，数据知识化和基于知识处理的未来信息服务业，低成本信息化和用信息技术提升传统产业，智能与认知科学、生物信息学、社会信息学等前沿交叉科学，信息科学基础理论，信息安全等几个未来信息科学技术重点发展领域的优秀科研成果。丛书力争起点高、内容新、导向性强，具有一定的原创性；体现出科学出版社“高层次、高质量、高水平”的特色和“严肃、严密、严格”的优良作风。

希望这套丛书的出版，能为我国信息科学技术的发展、创新和突破带来一些启迪和帮助。同时，欢迎广大读者提出好的建议，以促进和完善丛书的出版工作。

中国工程院院士
原中国科学院计算技术研究所所长
李国杰

序

量子理论是一个极为奇妙的理论，以至于引发了爱因斯坦和玻尔半个世纪的争论。量子信息科学是量子力学与信息学交叉形成的一门边缘学科。近年来，量子信息学给经典信息科学带来了新的机遇和挑战。量子特性在信息领域中有着独特的功能，在提高运算速度、确保信息安全、增大信息容量和提高检测精度等方面可能突破现有经典信息系统的极限。近年来，量子信息科学在理论和实验上已经取得了重要突破，引起各国政府、科技界和信息产业界的高度重视。因此，发展量子信息科学，发展我国信息安全事业，使我国在量子信息科学领域占有一席之地，实为当务之急。

杨宇光老师长期从事信息安全，特别是量子密码的研究工作，对量子密码有着深刻的理解。该书全面介绍了量子密码学，包括量子密码学的发展历史、量子密码学与量子计算的关系、量子密钥分发和身份认证、量子安全直接通信、量子秘密共享、量子签名、安全多方量子计算、量子密码协议的安全性分析方法以及量子密集编码等内容。

该书的撰写前后历时五年有余，反映了量子密码学的新发展和新趋势，并结合作者的最新科研成果，是一部符合时代需求的佳作。我相信，该书的出版将对我国信息安全理论的发展产生积极影响并作出重要贡献。

中国工程院院士

沈昌祥

2013 年 1 月

前　言

20 世纪初发生了两大物理学革命：相对论和量子力学。这两大革命把物理学的研究领域从经典物理学的宏观世界分别扩展到了宇观世界和微观世界。

量子特性在信息领域中有着独特的功能，在提高运算速度、确保信息安全、增大信息容量和提高检测精度等方面可能突破现有经典信息系统的极限，于是便诞生了一门新的学科分支——量子信息科学。它是量子力学与信息科学相结合的产物，包括量子密码、量子通信、量子计算等。近年来，在理论和实验上已经取得了重要突破，引起各国政府、科技界和信息产业界的高度重视。

在实验中任何两态量子系统都可以用来制备量子比特，常见的有光子的正交偏振态、电子或原子核的自旋、原子或量子点的能级、任何量子系统的空间模式等。信息一旦量子化，量子力学的特性便成为量子信息的物理基础，其主要有①量子态叠加性：量子信息可以同时输入或操作 N 个量子比特的叠加态；②量子相干性：量子干涉现象成为量子信息诸多特性的重要物理基础；③量子纠缠性：N(大于 1)个量子比特可以处于量子纠缠态，对其中某个子系统的局域操作会影响到其余子系统的状态；④量子不可克隆定理：量子力学的线性特性禁止对任意量子态实行精确的复制，这个定理和 Heisenberg 测不准原理构成量子密码学的物理基础。

随着 2008 年、2009 年国内基于已有商用光纤的光量子电话网、城域网络量子通信技术以及安徽芜湖量子政务网等量子通信网络的成功实现，国内在实用化量子通信方面取得了重大进展，绝对安全的量子通信由实验室走进了日常生活。从未来科技发展的领域看，随着量子通信技术的发展，光量子电话网、量子城域网以及量子政务网等量子通信网络的成功构建，通过商业光纤网络，多个用户之间可以进行真正安全、不怕任何窃听的量子通信，量子通信真正展现了它的应用价值。

著名计算机学家、计算机科学最高奖“图灵奖”获得者，清华大学姚期智院士指出量子网络是下一代互联网可供选择方案之一，并担任首席科学家启动了我国 973 重大科学问题导向项目“全量子网络”。在国际上，2011 年，加拿大量子计算公司 D-Wave 在量子计算机研究方面取得了重大突破，正式发布了全球第一款商用型量子计算机“D-Wave One”，量子计算机的梦想又近了一大步。

全书分为九章。第 1 章为绪论，主要介绍密码学和量子密码学的发展历史、量子密码学与量子计算的关系以及量子密码学面临的挑战和应用前景；第 2 章为量子安全通信研究所需的量子力学基础知识；第 3～9 章分别介绍了量子密码协议的设计和安全性分析方法，主要包括量子密钥分发和身份认证、量子安全直接通信、

量子秘密共享、量子签名、安全多方量子计算、量子密码协议的安全性分析方法以及量子密集编码。

本书以作者课题组近五年来的研究成果为主体，结合国内外学者在量子密码学领域的代表性成果，对这一领域的主要内容作了系统论述，并提出了一些新的研究课题及进展。

作者在此感谢实验室夏娟、贾鑫、滕义伟、柴海平、王宏洋、田举、徐鹏等研究生的部分工作，同时感谢科学出版社的魏英杰编辑的理解和支持。本书也得到了国家自然科学基金(项目编号：61003290)、北京市自然科学基金(项目编号：4122008、1102004)、2013 年度北京市属高等学校青年拔尖人才培育计划(CIT & TCD201304039)、科研基地—科技创新平台—可信系统研发(007000546612003)、学科与研究生教育—重点学科—信息安全(007000541212020)的资助。

由于时间紧迫，加之作者的水平所限，书中错误疏漏之处在所难免，不当之处希望广大读者批评指正。

作　者

2013 年 1 日

目　录

第1章 绪 论

密码学(Cryptology)源自希腊语“krypto‘s”及“logos”,直译即为“隐藏”及“消息”之意。密码作为一门技术源远流长,可以追溯到几千年前的远古战争时代。存于石刻或史书中的记载表明,许多古代文明,包括埃及人、希伯来人、亚述人都在实践中逐步发明了密码系统。从某种意义上说,战争是科学技术进步的催化剂。可以说人类自从有了战争,就有了密码。尤其是二战期间,密码研究曾经有过高度的繁荣。长期以来,密码技术总是和政治、经济、军事联系在一起。

1.1 密码学的发展历史

密码学的发展历程大致经历了古代加密方法、古典密码和现代密码等三个阶段。

1.1.1 古代加密方法(手工阶段)

古代加密方法大约起源于公元前440年,出现在古希腊战争中的隐写术。当时为了安全传送军事情报,奴隶主剃光奴隶的头发,将情报写在奴隶的光头上,待头发长长后将奴隶送到另一个部落,再次剃光头发,原有的信息复现出来,从而实现这两个部落之间的秘密通信。

公元前5世纪,古希腊斯巴达出现原始的密码器,称为斯巴达木卷。斯巴达木卷由一根木杖和一块缠绕在上面的丝绸构成。将信息沿着木杖的方向写在缠绕在木杖的丝绸上,然后展开丝绸。丝绸上面的文字顺序就变得杂乱无章了,信使会把这块丝绸传递给收信人。收信人收到后,找到一根直径相同的木杖,把丝绸缠上去,就可以读取信息了,这是最早的密码技术。

我国古代也早有以藏头诗、藏尾诗、漏格诗及绘画等形式,将要表达的真正意思或“密语”隐藏在诗文或画卷中特定位置的记载,一般人只注意诗或画的表面意境,而不会去注意或很难发现隐藏其中的“话外之音”。例如,

我画蓝江水悠悠,
爱晚亭上枫叶愁。
秋月溶溶照佛寺,
香烟袅袅绕经楼。

1.1.2 古典密码(机械阶段)

古典密码的加密方法一般是文字置换,使用手工或机械变换的方式实现。古典密码系统已经初步体现出现代密码系统的雏形,它比古代加密方法复杂,变化较小。古典密码主要有两大基本方法:代替密码(将明文的字符替换为密文中的另一种的字符,接收者只要对密文做反向替换就可以恢复出明文)、置换密码(明文的字母保持相同,但顺序被打乱了)。例如,著名的凯撒(Caesar)密码,公元前一世纪,著名的凯撒密码被用于高卢战争中,这是一种简单易行的单字母替代密码。凯撒只是简单地把信息中的每一个字母用字母表中该字母后的第三个字母代替,这种密码替换称为凯撒密码。

公元 9 世纪,阿拉伯的密码学家阿尔·金迪(al′Kindi),也被称为伊沙克(Ishaq),提出解密的频度分析方法,通过分析计算密文字符出现的频率破译密码。

公元 16 世纪中期,意大利的数学家卡尔达诺(Cardano),发明了卡尔达诺漏格板,覆盖在密文上,可以从漏格中读出明文,这是较早的一种分置式密码。

公元 16 世纪晚期,英国的菲利普斯(Philips)利用频度分析法成功破解苏格兰女王玛丽的密码信,信中策划暗杀英国女王伊丽莎白,这次的解密将玛丽送上了断头台。几乎在同一时期,法国外交官维热纳尔(Vigenere)提出著名的维热纳尔方阵密表和维热纳尔密码,这是一种多表加密的替代密码,可使阿尔·金迪和菲利普斯的频度分析法失效。

公元 1863 年,普鲁士少校卡西斯基(Kasiski)首次从关键词的长度着手将它破解。英国的巴贝奇(Babbage)通过仔细分析编码字母的结构也将维热纳尔密码破解。

公元 20 世纪初,第一次世界大战进行到关键时刻,英国破译密码的专门机构“40 号房间”利用缴获的德国密码本破译了著名的“齐麦曼电报”,促使美国放弃中立参战,改变了战争进程。

公元 1918 年,美国数学家吉尔伯特·维那姆发明一次性便笺(one-time pads)密码,它是一种理论上绝对无法破译的加密系统,被誉为密码编码学的圣杯。但产生和分发大量随机密钥的困难使它的实际应用受到很大的限制,从另一方面来说安全性也更加无法保证。

第二次世界大战中,在破译德国著名的恩格玛(Enigma)密码机密码过程中,原本是以语言学家和人文学者为主的解码团队中加入了数学家和科学家。电脑之父亚伦·图灵就是在这个时候加入了解码队伍,发明了一套更高明的解码方法。同时,这支优秀的队伍设计了人类的第一部电脑来协助破解工作。显然,越来越普及的计算机也是军工转民用产品。美国人破译了被称为“紫密”的日本“九七式”密码机密码。靠前者,德国的许多重大军事行动对盟军都不再成为秘密;靠后者,美

军炸死了偷袭珍珠港的元凶日本舰队总司令山本五十六。

在第二次世界大战中，印第安纳瓦约土著语言被美军用作密码。在第二次世界大战日美的太平洋战场上，美国海军军部让北墨西哥和亚利桑那印第安纳瓦约族人使用纳瓦约语进行情报传递。纳瓦约语的语法、音调及词汇都极为独特，不为世人所知道，当时纳瓦约族以外的美国人中，能听懂这种语言的也就一二十人。这是密码学和语言学的成功结合，纳瓦约语密码成为历史上从未被破译的密码。

1.1.3 现代密码(计算机阶段)

前面两种密码的研究还称不上是一门科学。直到1949年，香农发表了《保密系统的通信理论》，把密码学建立在严格的数学基础之上。密码学从此才成为真正意义上的科学。该文利用数学方法对信息源、密钥源、接收和截获的密文进行了数学描述和定量分析，提出了通用的秘密钥密码体制模型。

需要提出的是，由于受历史的局限，20世纪70年代中期以前的密码学研究基本上是秘密地进行，而且主要应用于军事和政府部门。密码学的真正蓬勃发展和广泛的应用是从70年代中期开始的。1977年美国国家标准局颁布了数据加密标准DES用于非国家保密机关。该系统完全公开了加密、解密算法，突破了早期密码学的信息保密的单一目的，使得密码学得以在商业等民用领域的广泛应用，从而给这门学科以巨大的生命力。

在密码学发展的进程中另一件值得注意的事件是，1976年美国密码学家迪菲和赫尔曼在题为《密码学的新方向》一文中提出了一个崭新的思想，不仅加密算法本身可以公开，甚至加密用的密钥也可以公开。但这不意味着保密程度的降低。如果加密密钥和解密密钥不一样，将解密密钥保密就可以。这就是著名的公钥密码体制。若存在这样的公钥体制，就可以将加密密钥像电话簿一样公开，任何用户当它想经其他用户传送一加密信息时，就可以从这本密钥薄中查到该用户的公开密钥，用它来加密，而接收者能用只有它所具有的解密密钥得到明文。任何第三者不能获得明文。1978年，美国麻省理工学院的里维斯特、沙米尔和阿德曼提出了RSA公钥密码体制，这是第一个成熟的、迄今为止理论上最成功的公钥密码体制。其安全性是基于数论中的大整数因子分解。

从这个意义上讲，如果人们能够在实际中实现“Shor大数因子化”的量子算法，RSA保密体制完成的任何加密就会被解密。因此，量子计算会对由传统密码体系保护的信息安全构成致命的打击，对现有保密通信提出了严峻挑战。另外，根据摩尔定律，计算机的运算速度每隔大约两年就会增长一倍，破译基于计算复杂性的密码的难度不断降低，密钥长度必须不断增长。作为基于数学复杂性的密码体制克星的量子计算机以及量子并行算法的研究热潮的到来，使得基于数学复杂性的密码体制的安全性岌岌可危，这迫使人们开始研究新的密码体制，如量子密码。