普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

教育部高等学校信息安全专业教学指导委员会
中国计算机学会教育专业委员会 共同指导

顾问委员会主任：沈昌祥 编委会主任：肖国镇

Post Quantum Cryptography
抗量子计算密码

Daniel J. Bernstein
Johannes Buchmann 编著
Erik Dahmen

张焕国 王后珍 杨昌 等译

http://www.tup.com.cn

Information Security

根据教育部高等学校信息安全专业教学指导委员会编制的
《高等学校信息安全专业指导性专业规范》组织编写

清华大学出版社 Springer

普通高等教育“十一五”国家级规划教材

高等院校信息安全专业系列教材

Post Quantum Cryptography

抗量子计算密码

Daniel J. Bernstein
Johannes Buchmann 编著
Erik Dahmen

张焕国 王后珍 杨昌 等译

Information Security

http://www.tup.com.cn

清华大学出版社
北京

图书在版编目（CIP）数据

抗量子计算密码/（美）伯恩斯坦（Bernstein，D. J.），（德）布赫曼（Buchmann，J.），（德）达门（Dahmen，E.）编著；张焕国，王后珍，杨昌等译. —北京：清华大学出版社，2015

高等院校信息安全专业系列教材

ISBN 978-7-302-36351-4

Ⅰ. ①抗… Ⅱ. ①伯… ②布… ③达… ④张… ⑤王… ⑥杨… Ⅲ. 电子计算机－密码术－高等学校－教材 Ⅳ. ①TP309.7

中国版本图书馆 CIP 数据核字(2014)第 287478 号

责任编辑：张 民 顾 冰

封面设计：何凤霞

责任校对：焦丽丽

责任印制：李红英

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 刷 者：三河市君旺印务有限公司

装 订 者：三河市新茂装订有限公司

经 销：全国新华书店

开 本：185mm×260mm **印 张**：13.25 **字 数**：305 千字

版 次：2015 年 2 月第 1 版 **印 次**：2015 年 2 月第1 次印刷

印 数：1～1500

定 价：29.50 元

产品编号：040496-01

高等院校信息安全专业系列教材

编审委员会

出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定，确定了本丛书首批教材的作者，这些作者绝大多数都是既在本专业领域有深厚的学术造诣、又在教学第一线有丰富的教学经验的学者、专家。

本系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整、结构合理、内容先进。

② 适应面广：能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套：除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

为了保证出版质量，我们坚持宁缺毋滥的原则，成熟一本，出版一本，并保持不断更新，力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材，满足学生用书的基础上，还经由专家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到本系列教

材中，以进一步满足大家对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍，同时也欢迎广大读者对本系列教材提出宝贵意见，以便我们对本系列教材的组织、编写与出版工作不断改进，为我国信息安全专业的教材建设与人才培养做出更大的贡献。

“高等院校信息安全专业系列教材”已于2006年年初正式列入普通高等教育“十一五”国家级教材规划（见教高[2006]9号文件《教育部关于印发普通高等教育“十一五”国家级教材规划选题的通知》）。我们会严把出版环节，保证规划教材的编校和印刷质量，按时完成出版任务。

2007年6月，教育部高等学校信息安全类专业教学指导委员会成立大会暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办，清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展起到重要的指导和推动作用。2006年教育部给武汉大学下达了“信息安全专业指导性专业规范研制”的教学科研项目。2007年起该项目由教育部高等学校信息安全类专业教学指导委员会组织实施。在高教司和教指委的指导下，项目组团结一致，努力工作，克服困难，历时5年，制定出我国第一个信息安全专业指导性专业规范，于2012年底通过经教育部高等教育司理工科教育处授权组织的专家组评审，并且已经得到武汉大学等许多高校的实际使用。2013年，新一届“教育部高等学校信息安全专业教学指导委员会”成立。经组织审查和研究决定，2014年以“教育部高等学校信息安全专业教学指导委员会”的名义正式发布《高等学校信息安全专业指导性专业规范》（由清华大学出版社正式出版）。“高等院校信息安全专业系列教材”在教育部高等学校信息安全专业教学指导委员会的指导下，根据《高等学校信息安全专业指导性专业规范》组织编写和修订，进一步体现科学性、系统性和新颖性，及时反映教学改革和课程建设的新成果，并随着我国信息安全学科的发展不断完善。

我们的E-mail地址：zhangm@tup.tsinghua.edu.cn；联系人：张民。

“高等院校信息安全专业系列教材”编审委员会

译者序

21世纪是信息的时代，除了电子信息科学技术继续高速发展之外，量子和生物等新型信息科学正在建立和发展。量子信息科学的研究和发展催生了量子计算机、量子通信和量子密码的出现。

由于量子信息的奇妙特性，使得量子计算具有天然的并行性。例如，当量子计算机对一个 n 量子比特的数据进行处理时，量子计算机实际上是同时对 2^n 个数据状态进行了处理。正是这种并行性使得原来在电子计算机环境下的一些困难问题，在量子计算机环境下却成为容易计算的。量子计算机的这种超强计算能力，使得基于计算复杂性的现有公钥密码的安全受到挑战。

目前可用于密码破译的量子计算算法主要有 Grover 算法和 Shor 算法。对于密码破译来说，Grover 算法的作用相当于把密码的密钥长度减少一半。而 Shor 算法则可以对目前广泛使用的 RSA、EIGamal、ECC 公钥密码和 DH 密钥协商协议进行有效攻击。这说明在量子计算环境下，RSA、EIGamal、ECC 公钥密码和 DH 密钥协商协议将不再安全。

早在 2001 年 IBM 公司就研制出 7 个量子位的示例型量子计算机，向世界宣告了量子计算机原理的可行性。2011 年 9 月 2 日，美国加州大学圣芭芭拉分校的科学家宣布，研制出具有冯·诺依曼计算机结构的量子计算机，并成功地进行了小合数的因子分解试验。2012 年 3 月 1 日 IBM 宣布找到了一种可以大规模提升量子计算机量子位数的关键技术。

除了美国之外，加拿大的量子计算机取得了长足的发展。2007 年 2 月加拿大 D－Wave System 公司宣布研制出世界上第一台商用 16 量子位的量子计算机。2008 年 5 月提高到 48 量子位。2011 年 5 月 30 日又提高到 128 量子位，并开始公开出售，1000 万美元一台。美国著名军火制造商洛克希德·马丁公司购买了这种量子计算机，用于新式武器的研制。2013 年初又大幅度地提高到 512 量子位，价格也上升为 1500 万美元一台。著名信息服务商谷歌公司购买了这种量子计算机，用于提高信息搜索效率和研究量子人工智能。

由上可知，量子计算机的发展大大超出了人们原来的预想。

必须指出的是，目前加拿大的量子计算机属于专用型量子计算机，它能够执行 Grover 算法，尚不能执行 Shor 算法。美国加州大学圣芭芭拉分校的量子计算机可以执行 Shor 算法，但量子位数太少。也就是说，目前的量子计算机尚不能对现有密码构成实际的威胁。但是，随着量子计算技术的发展，

总有一天会对现有密码构成实际威胁。

在量子计算环境下我们仍然需要确保信息安全，仍然需要使用密码，但是我们使用什么密码呢？这是摆在我们面前的一个重大战略问题。

根据哲学的基本原理，任何事物有优点，必然也有缺点。据此量子计算机有优势，必然也有劣势。有其擅长计算的问题，必然也有其不擅长计算的问题。

实际上，量子计算机能够有效攻击许多现有密码，但并不能有效攻击所有的现有密码。基于量子计算机不擅长计算的那些问题构造密码，就可以抵抗量子计算的攻击。我们称能够抵抗量子计算机攻击的密码为抗量子计算密码。

出于对抗量子计算密码需求的紧迫性，国际上从 2006 年开始举办"抗量子计算密码学术会议(Post-Quantum Cryptography)"，每两年举行一次，至今已举办了 4 届。已经产生了一批重要的研究成果，让人们看到了抗量子计算密码的新曙光。

为了使我国广大读者能够了解抗量子计算密码的发展，促进我国抗量子计算密码的科学研究和技术进步，清华大学出版社组织我们翻译出版了《抗量子计算密码》一书。

本书由 12 位作者供稿，并由其中的 3 位作者进行编著而成，这些作者都是抗量子计算密码领域各个分支的著名专家。本书系统地介绍了抗量子计算密码的基本原理、代表性成果和发展趋势。全书共分 6 篇，第 1 篇为抗量子计算密码导论。首先介绍量子计算机对现有密码的威胁，然后简单介绍现有抗量子计算密码的概貌，使读者对此领域有一个整体的了解。第 2 篇为量子计算。讲述了量子算法的工作原理及其最新进展，使读者能够对量子算法及其攻击密码的能力有一个了解。第 3 篇为基于 Hash 函数的数字签名方案。基于 Hash 函数的数字签名方案为抗量子计算密码提供了一种有趣的候选。本篇介绍了基于 Hash 函数的数字签名技术的发展，给出了几种代表性的方案。第 4 篇为基于纠错码的密码。纠错码是一种有效的容错技术，基于纠错码可以构造密码，而且具有抗量子计算攻击的能力。本篇介绍了基于纠错码的主要密码类型，并分析指出了它们的优缺点。第 5 篇为格密码。首先介绍了格的困难问题，然后介绍了几种有代表性的格密码。当前，格密码已成为学术界的研究热点。第 6 篇为多变量公钥密码学。多变量公钥密码被认为是能抵抗量子计算机攻击的公钥密码体制之一。本篇介绍了多变量公钥密码过去二十多年的发展和主要成果，并具体分析了每一种方案的优缺点。

本书内容丰富，较完整地给出了这一领域的全貌，不仅介绍现有成果，而且给出了今后的发展趋势。因此本书是一本很有参考价值的好书。本书可作为研究生和高年级本科生的教材或参考书，也可供从事信息安全、计算机、通信、数学、量子信息科学等领域的科技人员作为参考书。

本书的第 1 篇和第 4 篇由张焕国翻译，第 2 篇由杨昌翻译，第 3 篇由吴万青翻译，第 5 篇由毛少武翻译，第 6 篇由王后珍翻译。

本书的翻译采取了分工翻译，集体讨论修订的方法。博士研究生胡国香、王亚辉、刘金会、贾建卫等参与了翻译书稿的讨论修订和译稿整理工作。

由于译者的专业知识和外语水平有限，书中错误在所难免，敬请读者指正，译者在此先致感谢之意。

译者于武汉大学珞珈山

前言

第一届抗量子计算密码研讨会于2006年在Leuven的Katholieke大学举行。来自全世界的科学家们畅谈了量子计算和可以抵抗量子计算机攻击的密码方面的发展状况。大会报告人和与会听众一致认为，抗量子计算密码是一个有巨大吸引力的研究方向，如果大规模量子计算机被制造出来，那么对于今后的Internet来说抗量子计算密码将是决定性的关键技术。于是，我们决定编写一本关于抗量子计算密码的书。Springer出版社立即同意出版此书。我联系了几位在这一领域的顶级科学家，他们都愉快地接受了我的邀请。现在，我们很高兴地把这本书奉献给读者。我们希望本书能够成为介绍抗量子计算密码、纵览这一领域发展水平、鼓励更多科学家加入这一研究的一本图书。

我们要感谢编写本书的其他几位作者，与他们的合作是愉快的。我们还要感谢Springer出版社，特别是要感谢Ruth Alewelt和Martin Peters对我们的支持。首席编著者还要感谢Tanja Lange给予的关于抗量子计算密码的启蒙性的讨论，感谢学术界首先开始举办抗量子计算密码的系列研讨会。

Daniel J. Bernstein
Johannes A. Buchmann
Erik Dahmen
于芝加哥和达姆施塔特
2008年12月

贡献者列表

Daniel J. Bernstein
University of Illinois at Chicago
djb@cr. yp. to

Johannes Buchmann
Technische Universität Darmstadt
buchmann@cdc. informatik. tu-darmastadt. de

Erik Dahmen
Technische Universität Darmstadt
dahmen@cdc. informatik. tu-darmastadt. de

Jintal Ding
University of Cincinnati
ding@math. uc. edu

Sean Hallgren
The Pennsylvanis State University

Raphael Overbeck
EPFL, I&C, LASEC
Raphael. overbeck@epfl. ch

Oded Regev
Tel-Aviv University

Nicolas Sendrier
INRIA Rocquencourt
nicolas. sendrier@inria. fr

Michael Szydlo
Akamal Technologies
mike@szydle. com

Ulrich Vollmer
Berlin, Germany
ac@u. vellmer. name

Daniele Micciancio
University of California, San Diego
daniele@cs. ucsd. edu

Bo-Yin Yang
"Academia Sinica"
by@moscito. erg

目 录

第1篇 抗量子计算密码导论

Daniel J. Bernstein

University of Illinois at Chicago

1 密码学完蛋了吗

设想一下，从现在起的15年内的某一天，有人突然宣布研制出大规模量子计算机。《纽约时报》头版头条惊呼：所有用来保护Internet信息的公钥密码都被攻破了！用户们惊恐万状！密码学到底发生了什么灾难？

大概是当人们看到量子计算机攻破RSA、DSA和ECDSA密码后，便得出结论：密码学完蛋了！再也不能通过加密来保护信息，使攻击者不能读懂和不能伪造信息了。这意味着，要安全地存储信息和通信，只能使用昂贵的物理保护设备来阻止攻击者对信息的窃取。例如，可以把USB存储设备藏到一个上了锁的公文包里，并把公文包的链子套到一个可信的送信者的手腕上。

然而，最近的考察表明，从“量子计算机能攻破RSA、DSA和ECDSA密码”推出“量子计算机能彻底毁灭密码”的结论是没有根据的。除了RSA、DSA和ECDSA密码之外还有许多重要的密码是能够抵抗量子计算机攻击的。

- 基于Hash函数的密码　典型的例子是Merkle的Hash树公钥签名体制(1979年)。它是基于Lamport和Diffie的一次性消息签名思想构建的。
- 基于纠错码的密码　典型的例子是McEliece的基于Goppa码的公钥密码体制(1978年)。
- 基于格的密码　非常有趣的、具有吸引力的例子是Hoffstein-Pipher-Silverman的NTRU公钥加密体制(1998年)，但它不是第一个基于格的密码。
- 多变量二次方程组密码　一个最有趣的例子是Patarin的HFE^{v-}公钥签名体制(1996年)。它推广了Matsumoto和Imai的一个方案。
- 秘密钥密码　一个突出的例子是Daemen-Rijmen设计的Rijndael密码(1998年)。它后来被称为高级加密标准AES。

所有这些密码被认为是可以抵抗电子计算机攻击和量子计算机攻击的。目前，还没有人能给出一种用Shor算法攻击这些密码体制的有效方法。Shor算法是一种量子计算机求解离散对数问题的算法，它能够攻破RSA、DSA和ECDSA密码。另一种量子攻击

算法是 Grover 算法，它对这些密码体制都有一定的攻击作用。但是 Grover 算法没有 Shor 算法那样有效，密码技术人员可以通过简单地加长密钥来对付 Grover 算法的攻击。

是否存在一种更好的攻击方法攻击这些密码体制呢？应该是存在的。这是密码学上的常规性风险，这就是密码界为什么投入很大的时间和精力来进行密码分析的原因。如果密码分析者找到一种致命的攻击方法，就说明这种密码无用了。例如，对于 Merkle-Hellman 背包公钥加密体制，每一种可用的参数选择都容易被攻破。有时候密码分析者找到了并不致命的攻击方法，于是为了安全必须加大密钥的长度。有时候密码分析者研究很多年，都没能找到有所改进的攻击方法，于是密码界开始相信，最好的攻击方法已经找到，或者至少现实世界的攻击者不可能提出更好的攻击方法。

例如，考虑下面 3 种针对 RSA 的因子分解攻击方法：

- 1978 年，Rivest、Shamir 和 Adleman 在其原始论文中提到一个新算法，即 Schroeppel 的“线性筛法”。用它来分解 RSA 的模 n 并攻破 RSA 密码，需要计算 $2^{(1+o(1))(\lg n)^{1/2}(\lg\lg n)^{1/2}}$ 次基本运算，其中 lg 表示 $\lg_2$。假设“线性筛法”至少要用 2^b 次基本运算，则 n 至少要有 $(0.5+o(1))b^2/\lg b$ 位。

注意：$0.5+o(1)$ 意味着当 $b\to\infty$ 时收敛于 0.5。这并不能说明什么，例如 $b=128$。但是要根据 $b=128$ 算出合适的 n 的位数，就需要密切关注“线性筛法”的实际速度。

- 1988 年，Pollard 提出了一个新的分解算法，即“数域筛法”。用 Buhler，Lenstra 和 Pomerance 对它的一个重要扩展来分解 RSA 的模 n，需要计算 $2^{(1.9\cdots+o(1))(\lg n)^{1/3}(\lg\lg n)^{2/3}}$ 次基本运算。假设“数域筛法”至少要用 2^b 次基本运算，则至少要选择 n 有 $(0.016\cdots+o(1))b^3/(\lg b)^2$ 位。

今天看来，在 20 年后即使使用最快的因子分解算法利用传统的电子计算机进行因子分解，仍然需要计算 $2^{(\text{constant}+o(1))(\lg n)^{1/3}(\lg\lg n)^{2/3}}$ 次基本运算。这里的常数(constant)和 $o(1)$ 的细节可能会有某些改进，但是人们猜测 1/3 是最佳的，并且选择 n 的位数大约为 b^3 就可以抵抗电子计算机的所有可能的攻击。

- 1994 年，Shor 提出了一个因子分解算法。这个算法可以在 $(\lg n)^{1+o(1)}$ 量子位的量子计算机上，进行 $(\lg n)^{2+o(1)}$ 次基本运算，分解 RSA 的模 n。假设这个算法至少要用 2^b 次基本运算，意味着 n 至少要有 $2^{(0.5+o(1))b}$ 位。据此可知，对于任何有兴趣的 b，n 都是大的无法忍受的。关于量子算法的进一步内容，请参阅本书的“量子计算”一章。

为了对比，考虑对 30 年前 McEliece 提出的基于 Goppa 码的加密体制的攻击。McEliece 密码的原始论文中提出了一种攻击，要攻击长为 n，维数为 $n/2$ 的密码需要 $2^{(0.5+o(1))n/\lg n}$ 次基本运算。假设这个算法至少要用 2^b 次基本运算，就意味着 n 至少要有 $(2+o(1))b\lg b$ 位。后来的一些论文把攻击所需的基本运算数减少了很多，大约 $n^{\lg n}=2^{(\lg n)^2}$。但是如果 n 很大，则 $(\lg n)^2$ 远小于 $0.5n/\lg n$。于是，改进的攻击仍需要 $2^{(0.5+o(1))n/\lg n}$ 次基本运算。人们可以合理地猜测 $2^{(0.5+o(1))n/\lg n}$ 可能是最好的结果。看来量子计算机也不会有很大的不同，除非减小常数 0.5。

如果 McEliece 密码体制具有如此好的抗攻击能力，我们原先为什么不用它来替换