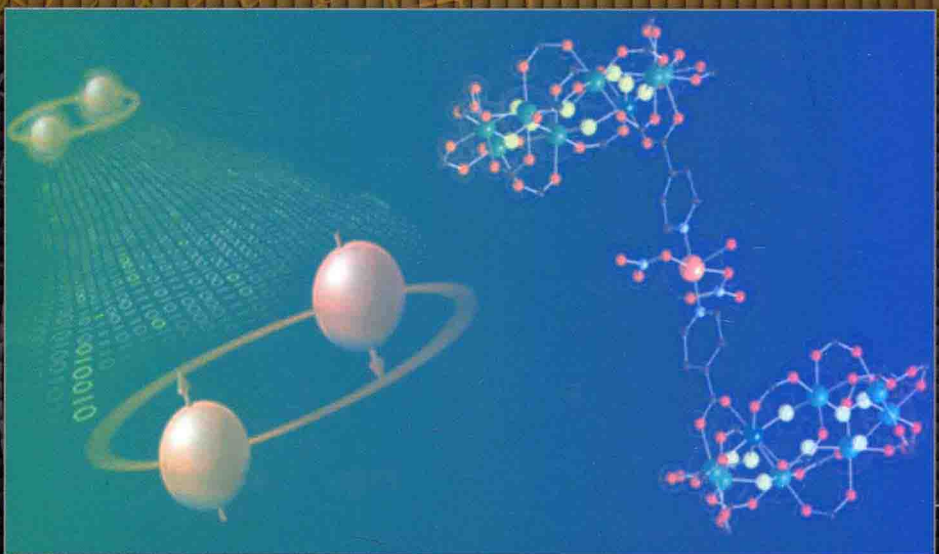
国防科技图书出版基金

网络与信息安全前沿技术丛书

密码前沿技术
——从量子不可精确克隆到DNA完美复制

陈晖 霍家佳 徐兵杰 张文政 编著

New Directions in Cryptography
—From quantum no cloning to DNA's perfect reproducing



国防工业出版社
National Defense Industry Press

国防科技图书出版基金

网络与信息安全前沿技术丛书

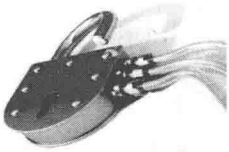
陈 晖 霍家佳 徐兵杰 张文政 编著

密码前沿技术

——从量子不可精确克隆到DNA完美复制

New Directions in Cryptography

—— From quantum no cloning to DNA's perfect reproducing



密码技术的发展不是以创建深奥的新理论为目的，而是致力于发掘具有内在安全特性的数据加密保护手段或途经，为国家、企业团体或个人提供重要或敏感数据的加密保护。量子密码、抗量子计算的密码、DNA密码等是人们新发现的有望为密码应用创新注入新活力的几个热点技术方向。本书力求从科普的角度为广大读者提供一个了解这些密码技术最新动态的新视角，为网络与信息安全、量子信息和生物信息等技术领域的专家、学者和工程技术人员等提供有价值的技术参考。

国防工业出版社
National Defense Industry Press
·北京·

图书在版编目(CIP)数据

密码前沿技术：从量子不可精确克隆到DNA完美复制/陈晖等编著. —北京：国防工业出版社，2015.6
（网络与信息安全前沿技术丛书）
ISBN 978-7-118-10136-2

Ⅰ.①密… Ⅱ.①陈… Ⅲ.①密码-研究 Ⅳ.①TN918.2

中国版本图书馆CIP数据核字(2015)第139718号

※

国防工业出版社出版发行
（北京市海淀区紫竹院南路23号 邮政编码100048）
三河市众誉天成印务有限公司
新华书店经售
*
开本710×1000 1/16 印张14½ 字数260千字
2015年6月第1版第1次印刷 印数1—3000册 定价86.00元

国防书店：(010)88540777 发行邮购：(010)88540776
发行传真：(010)88540755 发行业务：(010)88540717

致 读 者

本书由国防科技图书出版基金资助出版。

国防科技图书出版工作是国防科技事业的一个重要方面。优秀的国防科技图书既是国防科技成果的一部分，又是国防科技水平的重要标志。为了促进国防科技和武器装备建设事业的发展，加强社会主义物质文明和精神文明建设，培养优秀科技人才，确保国防科技优秀图书的出版，原国防科工委于1988年年初决定每年拨出专款，设立国防科技图书出版基金，成立评审委员会，扶持、审定出版国防科技优秀图书。

国防科技图书出版基金资助的对象是：

1. 在国防科学技术领域中，学术水平高，内容有创见，在学科上居领先地位的基础科学理论图书；在工程技术理论方面有突破的应用科学专著。

2. 学术思想新颖，内容具体、实用，对国防科技和武器装备发展具有较大推动作用的专著；密切结合国防现代化和武器装备现代化需要的高新技术内容的专著。

3. 有重要发展前景和有重大开拓使用价值，密切结合国防现代化和武器装备现代化需要的新工艺、新材料内容的专著。

4. 填补目前我国科技领域空白并具有军事应用前景的薄弱学科和边缘学科的科技图书。

国防科技图书出版基金评审委员会在总装备部的领导下开展工作，负责掌握出版基金的使用方向，评审受理的图书选题，决定资助的图书选题和资助金额，以及决定中断或取消资助等。经评审给予资助的图书，由总装备部国防工业出版社列选出版。

国防科技事业已经取得了举世瞩目的成就。国防科技图书承担着记载和弘扬这些成就，积累和传播科技知识的使命。在改革开放的新形势下，原国防科工委率先设立出版基金，扶持出版科技图书，这是一项具有深远意义的创举。此举势必促使国防科技图书的出版随着国防科技事业的发展更加兴旺。

设立出版基金是一件新生事物，是对出版工作的一项改革。因而，评审工作需

要不断地摸索、认真地总结和及时地改进，这样，才能使有限的基金发挥出巨大的效能。评审工作更需要国防科技和武器装备建设战线广大科技工作者、专家、教授，以及社会各界朋友的热情支持。

让我们携起手来，为祖国昌盛、科技腾飞、出版繁荣而共同奋斗！

国防科技图书出版基金
评审委员会

国防科技图书出版基金
第七届评审委员会组成人员

主任委员	潘银喜			
副主任委员	吴有生	傅兴男	杨崇新	
秘书长	杨崇新			
副秘书长	邢海鹰	谢晓阳		
委员 （按姓氏笔画排序）	才鸿年	马伟明	王小谟	王群书
	甘茂治	甘晓华	卢秉恒	巩水利
	刘泽金	孙秀冬	芮筱亭	李言荣
	李德仁	李德毅	杨　伟	肖志力
	吴宏鑫	张文栋	张信威	陆　军
	陈良惠	房建成	赵万生	赵凤起
	郭云飞	唐志共	陶西平	韩祖南
	傅惠民	魏炳波		

《网络与信息安全前沿技术丛书》编委会

丛书序

网络的触角正伸向全球各个角落，高速发展的信息技术已渗透到各行各业，不仅推动了产业革命、军事革命，还深刻改变着人们的工作、学习和生活方式。然而，在人们享受信息技术带来巨大利益的同时，一次又一次网络信息安全领域发生的重大事件告诫人们，网络与信息安全已直接关系到国家安全和社会稳定，成为我们面临的新的综合性挑战，没有过硬的技术，没有一支高水平的人才队伍，就不可能在未来国际博弈中赢得主动权。

网络与信息安全是一门跨多个领域的综合性学科，涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等。“道高一尺、魔高一丈”，网络与信息安全技术在博弈中快速发展，出版一套覆盖面较全、反映网络与信息安全方面新知识、新技术、新发展的丛书有着十分迫切的现实需求。

适逢此时，欣闻由我国网络与信息安全领域著名专家何德全院士任编委会主任，以国家保密通信重点实验室为核心，集聚国内信息安全界知名专家学者，潜心数年编写的《网络与信息安全前沿技术丛书》即将分期出版。丛书有如下特点：一是全面系统。丛书涵盖了密码理论与技术、网络与信息安全基础技术、信息安全防御体系，以及近年来快速发展的大数据、云计算、移动互联网、物联网等方面的安全问题。二是适应面宽。丛书既很好地阐述了相关概念、技术原理等基础性知识，又较全面介绍了相关领域前沿技术的最新发展，特别是凝聚了作者

们多年来在该领域从事科技攻关的实践经验，可适应不同层次读者的需求。三是权威性好。编委会由我国网络和信息安全领域权威专家学者组成，各分册作者又均为我国相关领域的知名学者、学术带头人，理论水平高，并有长期科研攻关的丰富积累。

我认为该丛书是一套难得的系统研究网络信息安全技术及应用的综合性书籍，相信丛书的出版既能为公众了解信息安全知识、提升安全防护意识提供很好的选择，又能为从事网络信息安全人才培养的教师和从事相关领域技术攻关的科技工作者提供重要的参考。

作为特别关注网络信息安全技术发展的一名科技人员，我特别感谢何德全院士等专家学者为撰写本书付出的艰辛劳动和做出的重要贡献，愿意向读者推荐该套丛书，并作序。

前言

在信息技术日新月异的今天，人们的生活越来越依赖网络空间，个人隐私和国家安全相关数据广泛分布于网络空间，但是网络空间的数据安全状况并没有得到有效提升。例如，利用电磁波接收器窃取数据的技术门槛和成本越来越低，针对有线网络的搭线窃听也已经没有技术瓶颈，木马、病毒不断侵蚀网络系统终端，从无序大数据中提炼敏感信息的技术方兴未艾。

实际上，在高度互联互通的网络空间，获取数据几乎是一件随心所欲的事情。全世界上百颗军事卫星全天候地扫描记录地面态势，遍布每一个区域的视频监控系统全天候记录所有市民的行踪，越来越多的网络公司毫无遗漏地记录网民的访问数据，人们获取和存储的数据正在以指数级增长。毫无疑问，人们已经进入了大数据主导的时代。对于拥有大数据和超级计算资源的国家机构和互联网公司而言，监控变得轻而易举和随心所欲。搜索引擎网站可能最先知道其用户的奇思妙想，网络公司可以准确预测某个国家的社会、经济和科技发展状态与趋势等。这些事实充分说明，在大数据时代，数据安全将面临非常严峻的形势，而数据保护的核心技术——密码技术——也面临着越来越多的挑战。

为什么存储在计算机上的个人信息会被他人轻易窃取？其主要原因是个人信息是具有明确特征的格式化的数据，而不是具有内在随机性的数据，并且往往处于无任何有效保护的状态。实际上，大多数人对个人数据的安全态势缺少清晰的认识，并且为了方便，对个人信息很少采用合乎安全要求的保护。例如，登录口令简单化，对网络“钓鱼”和入侵缺少有效的防范，从而给日益泛滥的网络“黑客”以可乘之机。那么，为什么政府和军事保密通信数据会被破解？为什么采用标准加密算法加密的数据会被破解？其中的原因也是多方面的，而主要原因是密码的安全强度与密码破译能力的较量，这也是密码技术不断向前发展的内在动力。

在公元前5世纪，古希腊的斯巴达人将皮条紧紧缠绕在特定尺寸的木

棍子上，再把密信自上而下地写在皮条上，然后再把皮条解开并通过信使送给接收者。皮条的接收者只需要把皮条重新缠绕在相同尺寸的木棍上，就可以读出其中的信息。而在不知道木棍尺寸的情况下，这些皮条上的字母是杂乱无章的，由此达到保密通信的目的。这就是有记载的最早使用的保密通信器械——“天书”。在1412年盖勒·盖尚迪所编写的百科全书中，出现了多种移位密码和代替密码方案，通过打乱秘密信息的自然顺序达到保密的目的，这种保护手段在当时可能是有效的。但是替换密码并没有破坏英文语言的统计特性，因此利用统计分析方法可以快速破译。1883年，Auguste Kerckhoffs在《军事密码学》中提出一个重要的观点，即只有密码破译者才确切知道一个密码算法的安全性。1897年，马可尼发明了无线通信，这种新型的通信方式极大地促进了密码学的发展和成熟。在第一次世界大战中，密码分析在美国对德国宣战事件中起了十分重要的作用；在第二次世界大战中，密码分析在中途岛海战、阻击山本五十六等重要战役中也起到了非同小可的关键作用。密码通信以及密码分析在军事中的重要作用极大地促进了世界各国对密码技术研究的投入，从而为现代密码学的发展奠定了坚实的基础。

在第二次世界大战期间服务于美军情报机关的Shannon于1948年在《贝尔系统技术杂志》上发表了划时代的论文“通信的数学理论”。1949年他又发表了“保密系统的通信理论”，这就是Shannon的两篇里程碑式的论文，前者发展成为信息论，后者从信息论的观点对通信保密问题进行了系统的阐述，并奠定了现代密码学的信息论基础。

在Shannon信息论影响下，在20世纪70年代以后出现了诸如DES、RSA、MD5、AES等许多优秀的密码算法，为电子商务、电子政务等领域的信息安全做出了重要贡献。但是，随着计算技术和密码分析技术的快速发展，目前利用网格计算就可以在较短的时间内破译许多密码方案，这对商务、金融、政务等领域的信息安全构成了很大的威胁。近几年来，一向被认为安全的单向压缩函数MD5、SHA－0等被证实存在安全隐患，这进一步强化了人们对经典密码安全性的忧虑，目前广泛使用的安全性并未得到完备证明的数学密码体制很可能会在人们意想不到的时候被破译或者被发现存在致命安全漏洞等。另外，量子计算也给经典密码体制带来了前所未有的潜在挑战。

高性能并行计算能力的快速增长，特别是量子计算和DNA计算等并行计算算法的提出，为密码学研究进入下一阶段注入了新的强劲动力。根据已经发现的量子计算方法分析，目前的密码算法体系很难应对量子并行计算的攻击。一旦量子计算机投入使用，目前广泛使用的密码算法体系将面临更新换代的必然选择。然

而，新一代密码算法体系是否是经典密码算法的进一步完善？安全性基于计算复杂度的经典密码算法是否已经走到终点？目前，还很难对这些问题的解决列一个时间表，但是，具有物理安全性的新型密码算法已经走进人们的视野，目前量子密码和 DNA 密码已经成为密码前沿技术的代表，特别是量子密码已经具有比较广泛的实验基础。

密码前沿技术是一个十分宽泛的研究课题，覆盖面非常大，很难系统全面地对每一个新型密码技术进行详细介绍。因此，根据我们长期从事量子密码和 DNA 密码研究的成果，从量子不可精确克隆特性到 DNA 完美复制特性在密码技术中的应用，详细介绍这两类完全不同的物理安全密码新技术的基础理论、相关应用成果等，以期从科普的角度为读者提供一个新颖的研究视角。因此，本书不需要特别的数学、量子力学或生物学基础。另外，需要说明的是，量子信息和 DNA 技术都是比较活跃的前沿技术研究领域，其中包括许多重要的研究内容（如量子调控、量子传感、量子计算机、生物传感和生物智能等），而密码新技术只是其中一个热点研究内容。

由于作者水平有限，时间仓促，书中难免存在疏漏和不足，恳请专家、学者和读者批评指正。

编 者

2015 年 6 月于成都

目　录

第一篇　量子密码与抗量子计算密码