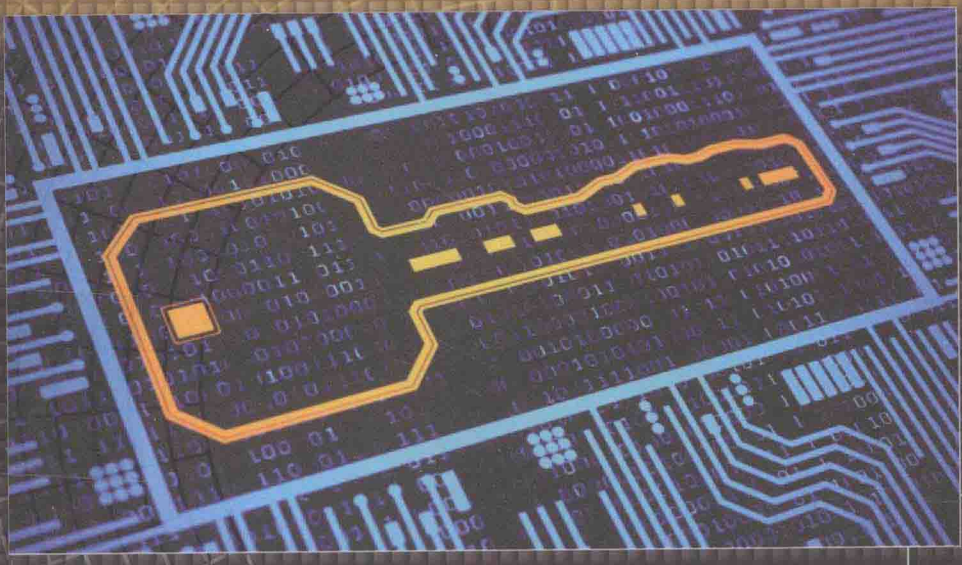
国防科技图书出版基金

网络与信息安全前沿技术丛书

随机数发生器及其在密码学中的应用

申兵　董新锋　徐兵杰　周宇　编著

Random Number Generators and Their Applications in Cryptography



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

申　兵　董新锋
徐兵杰　周　宇　编著

随机数发生器及其在密码学中的应用

Random Number Generators and Their Applications in Cryptography

随机数发生器只是密码产品中的“一丁点”组件，但却是最重要的部分，是安全的源头，若设计不当，则可能成为信息安全系统的“阿喀琉斯之踵”。如果您是密码工程师，希望本书能指导您设计或者正确使用安全的随机数发生器；如果您是密码理论工作者，希望本书能引导您进入密码学理论的殿堂，因为随机数发生器也是密码学理论的基石。

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

图书在版编目(CIP)数据

随机数发生器及其在密码学中的应用 / 申兵等编著.
—北京：国防工业出版社，2016.12
（网络与信息安全前沿技术丛书）
ISBN 978-7-118-11042-5

Ⅰ. ①随… Ⅱ. ①申… Ⅲ. ①密码学-研究②计算机安全-加密技术-研究 Ⅳ. ①TN918.1②TP309.7

中国版本图书馆 CIP 数据核字(2017)第 011218 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）
北京嘉恒彩色印刷有限责任公司
新华书店经售
*
开本 710×1000　1/16　**印张** 17　**字数** 322 千字
2016 年 12 月第 1 版第 1 次印刷　**印数** 1—3000 册　**定价** 86.00 元

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	赵伯桥	
秘书长	赵伯桥			
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。

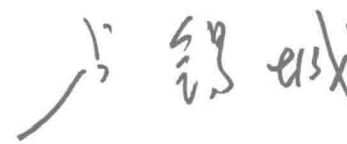
网络与信息安全是一门跨多个领域的综合性学科，涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等。“道高一尺、魔高一丈”，网络与信息安全技术在博弈中快速发展，出版一套覆盖面较全、反映网络与信息安全方面新知识、新技术、新发展的丛书有着十分迫切的现实需求。

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

互联网、移动通信、移动互联网、物联网……，网络已经改变了人类生活，这种改变还在继续且越来越深刻，如电子邮件取代传统信函，电子图书馆取代传统图书馆，网上支付成为重要的支付手段，社交网络流行等，网络已经深入到人类社会生活的方方面面。

随之而来的是网络中海量信息的安全问题，据估算，2013 年全球因网络安全问题导致的经济损失大约为 5000 亿美元，网络安全已经成为国家安全的一部分，习近平主席在 2014 年指出，没有网络安全就没有国家安全，网络安全已上升到国家战略。

从技术上讲，网络信息安全主要包含信息的机密性、完整性、可鉴别性、不可抵赖性，以及访问控制等。实现它们的重要手段是密码技术，主要包括对称加密、非对称加密、数字签名、数据完整性鉴别等，这些技术的一个共同之处，就是要实现“随机化”，例如，将具有明显意义的明文加密后，变成未授权者“无法读懂”的随机乱码，随机性是衡量一种密码技术是否“合格”的最基本的准则。另一方面，这些密码技术随机化的最终来源为密钥、初始向量，以及其他数据等，这些都必须是密码学安全的随机数，一旦被敌手识别并加以利用，即使是安全的密码技术也是空谈。再有，密码学作为一门学科，其自身的理论基础也和随机数（或者随机数发生器）紧密相连，如单向函数、伪随机置换、零知识证明等一些理论分支，都是建立在随机数发生器的基础上的，随机数发生器是密码学理论的基石。

由此可以看出，随机数不论在密码工程还是密码理论方面，都有着重要的作用，不可替代，但与密码算法、密码协议相比，随机数发生器只是密码产品中的“一丁点”组件，显得微不足道，也没引起学术界的重视，到目前为止，国内专门论述密码学随机数及其产生方法的专著未见出版。

出于这样的考虑，本书将从密码学的角度详述密码学随机数的理论、构造及其应用，主要包括两方面：一是密码工程方面，包括从第 4 章到第 8 章的内容，这是本书的重点，目的是供广大密码工程人员参考；二是密码理

论方面，由于这方面涉及较多的计算复杂度理论，理论性较强，所以只用一章的篇幅（见第3章）做概要介绍。具体地，各章安排如下：

第1章概述随机数在信息社会的重要作用、随机数的简要历史，并给出随机数的非形式化定义。

第2章从密码技术的各个方面，论述随机数和保密通信的密切关系，并给出熵的定义，这是随机性的量化指标，也是后续章节所要用到的一个基本概念和工具。

第3章为伪随机数发生器的理论，从计算复杂度的角度定义密码学伪随机数发生器，给出其存在性、构造方法等，作为理论上的直接应用，本章最后给出理论上利用伪随机数发生器构造伪随机函数（置换）的方法。

第4章论述满足工程需要的伪随机数发生器，它是用得最多的发生器，原则上，密码算法或者密码函数都可以用来构造实用的伪随机数发生器，所以本章的内容比较丰富，首先列出了密码学常用的伪随机数发生器的组件——线性反馈移位寄存器，然后列出了基于分组密码、序列密码构造伪随机数发生器的方法，接着介绍一个专用的伪随机数发生器 Yarrow，这是学术界为数不多的发生器之一，本章的最后介绍几个伪随机数发生器标准，包括 ANSI X9.17、FIPS 186 和美国国家标准与技术研究院（NIST）颁布的 SP800－90 中伪随机数发生器设计指南。

第5章为非确定随机数发生器，这类发生器主要用于产生真随机数，本章主要论述设计原理和评估方法，作为示例，最后介绍两个著名的真随机数发生器，一个是/dev/random，另一个是 Intel 随机数发生器。

第6章为量子随机数发生器，它本来是属于非确定性发生器这一类，但由于量子的特殊性和它在构造发生器上的天然优势，所以单列一章，详细介绍。首先介绍两类量子真随机数发生器，然后详细描述其具体的设计方法。

第7章为随机性的统计检验，对一段序列或者是一个随机数发生器，还没有一个从理论上证明其是随机的方法，所以随机性检验成了检测一个序列是否随机的重要方法，在工程上被广泛使用。首先给出了随机性检验的一般性方法，然后介绍目前流行的四种随机性检验包，最后是密码函数的随机性检验方法。

第8章为随机数发生器的分析方法，由于学术界研究不多，相关文献较少，所以只做概要介绍，主要包括攻击分类、微软 Windows 操作系统的随机数发生器的攻击实例，以及 SP800－90 中 Dual_EC_PRNG 的陷门分析。

本书的第1～3、5、8章主要由申兵编写，第4章由申兵和周宇共同编写，第6章由徐兵杰编写，第7章由董新锋编写。

保密通信重点实验室的朱甫臣研究员对手稿进行了全面仔细的审核，提出了

宝贵的意见和建议，在此表示衷心的感谢！全书的编写工作得到了中国电子科技集团公司第三十研究所和保密通信重点实验室的领导和同仁的大力支持，在此一并表示衷心的感谢！最后特别感谢国防工业出版社王晓光编辑认真、翔实、全面的核对和对该书付出的精心指导！

由于编者水平有限，时间仓促，书中难免存在不妥之处，恳请读者批评指正。

作 者

2016 年 10 月 10 日

目　录