现代密码分析学

——破译高级密码的技术

MODERN CRYPTANALYSIS

TECHNIQUES FOR ADVANCED CODE BREAKING

(美) Christopher Swenson 著
黄月江 祝世雄 等 译
张文政 校

国防工业出版社
National Defense Industry Press
WILEY

装备科技译著出版基金资助

现代密码分析学
——破译高级密码的技术

Modern Cryptanalysis
Techniques for Advanced Code Breaking

（美）Christopher Swenson 著
黄月江 祝世雄 等译
张戍[illegible] 校

WILEY
Wiley Publishing, Inc.

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

著作权合同登记　图字：军－2012－010号

图书在版编目(CIP)数据

现代密码分析学：破译高级密码的技术／(美)斯文森(Swenson,C.)著；黄月江，祝世雄译. —北京：国防工业出版社，2012.11

书名原文：Modern Cryptanalysis：Techniques for Advanced Code Breaking

ISBN 978－7－118－08132－9

Ⅰ. ①现... Ⅱ. ①斯... ②黄... ③祝... Ⅲ. ①密码术 Ⅳ. ①TN918.3

中国版本图书馆 CIP 数据核字(2012)第231314号

Translation from the English Language edition:
MODERN CRYPTANALYSIS: TECHNIQUES FOR ADVANCED CODE BREAKING by Christopher Swenson
ISBN 978－0－470－13593－8

10475 Crosspoint Boulevard
Indianapolis, IN46256

※

國防工業出版社出版发行
(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710×960　1/16　印张14¼　字数243千字
2012年11月第1版第1次印刷　印数1—2000册　定价60.00元

(本书如有印装错误，我社负责调换)

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

现代密码分析学
——破译高级密码的技术

威利出版公司出版
印第安纳波利斯,IN46256,
克拉斯颇因特大街 10475 号

由美国印第安纳州印第安纳波利斯市威利出版公司与加拿大联合发行
ISBN: 978-0-470-13593-8
于美国印刷(制作)
10 9 8 7 6 5 4 3 2 1

此引起的损失负责。在本书中,将一个组织或网站作为进一步信息的引用和/或进一步信息的潜在来源这一事实并不意味作者或出版者对组织或网站可能提供的信息作保证或者对它(们)可能作的推荐作保证。另外,读者应当意识到在写本书和读本书的时候,本书中列出的互联网网站可能已经变化或消失。

为了得到有关我们其他作品和服务的一般信息或为了得到技术支持,请在美国国内通过(800)762 - 2974 和我们的顾客管理部联系,在美国之外通过(317)572 - 3993 或传真(317)572 - 4002 和我们的顾客管理部联系。
从出版者那里可得国会图书馆出版目录分类数据。

本书表达的观点和意见并不反映美国国防部的观点与意见。

译者序

在信息社会里，无论国家、单位还是个人都越来越认识到信息安全的重要性，而密码学是信息安全的基础，几乎所有的信息系统都使用了密码技术。对一个使用了密码技术的系统来说，首先要保证系统的安全性，即所使用的密码体制是安全的；其次，对一个加了密的“敌对”系统，应想方设法地去破译该系统，破译该系统的核心最终都归结到密码体制的破译，所以掌握常见的密码体制的破译方法，对设计和破译密码算法是非常必要的。目前国内、外已有很多介绍密码学的书籍，但密码破译分析学方面的专著甚少。本书的作者 Christopher Swenson 博士在密码分析方面做出了出色的研究成果，曾获得由国际密码研究协会（IACR）和美国数学学会（AMS）共同颁发的信息安全学术成就奖。Christopher Swenson 博士在本书中全面、系统地介绍了密码分析学，有助于我们学习国外最新的密码分析技术，了解我们与国际先进水平之间的差距，推动我国密码分析技术的发展。

本书有如下特点：

1. 内容丰富。全面地介绍了古典密码、公钥密钥和分组密码的分析方法，并将这些方法应用于当前流行的密码算法的分析。

2. 自成体系。给出了学习这些分析方法所必需的数学知识，并用有趣的例子去帮助读者进行理解。习题的良好设计也能使读者更深入地体会所讲述的方法。

3. 理论前沿。不仅总结了通用的分析方法，而且还介绍了许多最新的分析技术，如差分分析及其变型、线性分析和飞去来器攻击等。

本书还系统、全面地介绍了密码分析学领域的重要参考文献，是一本可读性强和详细描述当代密码分析学现状的著作。本书的出版，希望能对国内从事信息安全和密码分析的同行们提供借鉴和帮助，也可作为信息安全专业的研究生以及相关专业的大学高年级本科生全面学习密码分析理论的基础性书籍，可供从事密码设计和破译工作的科研人员参考。

全书由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共同翻译完成，国防工业出版社王晓光编审为本书的顺利出版给予了悉心指导和辛苦努力。以下人员参与了出版、翻译和审校工作：黄月江、祝世雄、张文政、曾兵、霍家佳、谯通旭、赵伟、王林、于飞、张李军、周宇、董新锋、范佳、周文、张雅念、张晓玉等，在此对他们辛勤的工作表示衷心的感谢！

由于译者水平有限，书中难免会有一些错误和不当之处，欢迎读者批评指正！

译 者

2012 年 4 月

作 者 简 介

克里斯托弗·斯文森(邮箱：www. caswenson. com)现正在塔尔萨大学攻读计算机科学博士学位，而且他还在该校协助并教授信息安全课程、电信学课程和密码分析课程。他是积极的研究者并已发表了多篇安全领域的论文。他获得了信息保障奖学金，该项目即国防部赛博部队项目。

原书编辑人员

执行编辑
卡罗尔·朗

开发编辑
约翰·斯里维尔

制作编辑
迪部尔·班利杰尔

复制编辑
卡特·卡夫瑞

编辑经理
玛丽·贝斯·瓦克菲尔德

制作经理
蒂姆·塔特

副社长兼执行集团出版者
理查德·斯瓦德利

副社长兼执行出版者
约瑟夫 B. 维克特

设计协调人,封面
林瑟·斯坦福

校对人员
南希·卡南斯科

编索引人员
莫兰尼·贝尔金

封面图像
ⓒ雅玛达·塔罗/数字影像/盖特图像

致　谢

我感谢帮助我出版本书的许多人士。首先，感谢我的未婚妻瑟斯德·布拉姆，她在本书的写作过程中一直支持我。我要感谢苏吉特·舍诺依和塔尔萨大学，他们为我提供场地以便教授原创性课程（还要感谢学习该课程的所有学生）。当然，我要感谢我的母亲格冷达和我的父亲罗杰，以及我的姐妹瑞克和杰西，还有我的继父理查德，他们这么多年来一直支持我。

没有威利出版公司的卡罗尔· 朗和约翰·斯里维尔的支持我不可能写出本书。还要非常感谢唐纳德·克鲁斯，莱斯利·南颇特和约翰·霍比，以及数以百计的人员，他们在 TeX、LaTeX、MetaPost 和相关的排字项目上付出了努力。

目 录

引　言

正如许多事情一样，在密码分析学领域没有一本教科书介绍现代密码学的进展，本书对这个问题给出了回答。密码分析学在最近的数百年中已经得到了长足的发展，人们对密码分析学进行了广泛的研究并得到了大量成果。

然而，当我们进入20世纪后，这些密码分析学的书籍和资料变得相对滞后。每一本“密码分析学”方面的书几乎都是100年以前的，按今天的标准，这些书主要关注某些最简单密码的破译。

相反，这个领域本身并没有停止发展，特别是在刚刚过去的30年里，随着日益强大的计算机的出现，它得到了难以置信的快速研究。在世界范围内，在密码分析学方面举办了各种会议和出版了许多论文，但没有人去考虑借助一种简单的方式来让人们去从头开始学习密码分析学。Bruce Schneier在文献[5]中已经指出这种方式是不值得的，因为这个领域变化得太快了，他的话极有道理。但是，当前密码分析学上的方法都是建立在相同的基础上的，并且大多数背景资料都需要懂得当前的研究情况或者参与到其中，这些将使学习变得越来越庞大和复杂。更重要的是，一些重要的论文都是由不同的人群和出于不同的个人目的而写的，这些使得人们理解起来更困难。

但我必须重申Schneier在文献[5]中说过的话：仅仅有一种方式能使得人们成为一个好的密码分析专家——练习破译密码。然而，我希望这本书能使新的或熟练的密码分析学家全面了解许多密码分析方面的成果。

当我在塔尔萨大学教学时，许多同学对密码分析学表现出了极大的兴趣，他们知道我喜欢该领域。我开始准备这门课，尽管我使用的是参考文献[7]，但是我还是发现没有一本我真正想要的教科书。

为此我开始从各种会议和出版物中收集各种材料，而且为学生整理上课中的各种笔记和摘要。同时我意识到也许有其他几个人与我有同样的问题：在较少的理论基础上想自学这个学科，甚至教学和上课。我们希望有这些人，否则将使我的出版商对推销这本书非常失望。

为了适当地讲现在密码分析学，我们不得不先做一些其他的事：最重要的是商定要做的和为什么要去做，这些就是引言中要介绍的。尽管我会把更有力