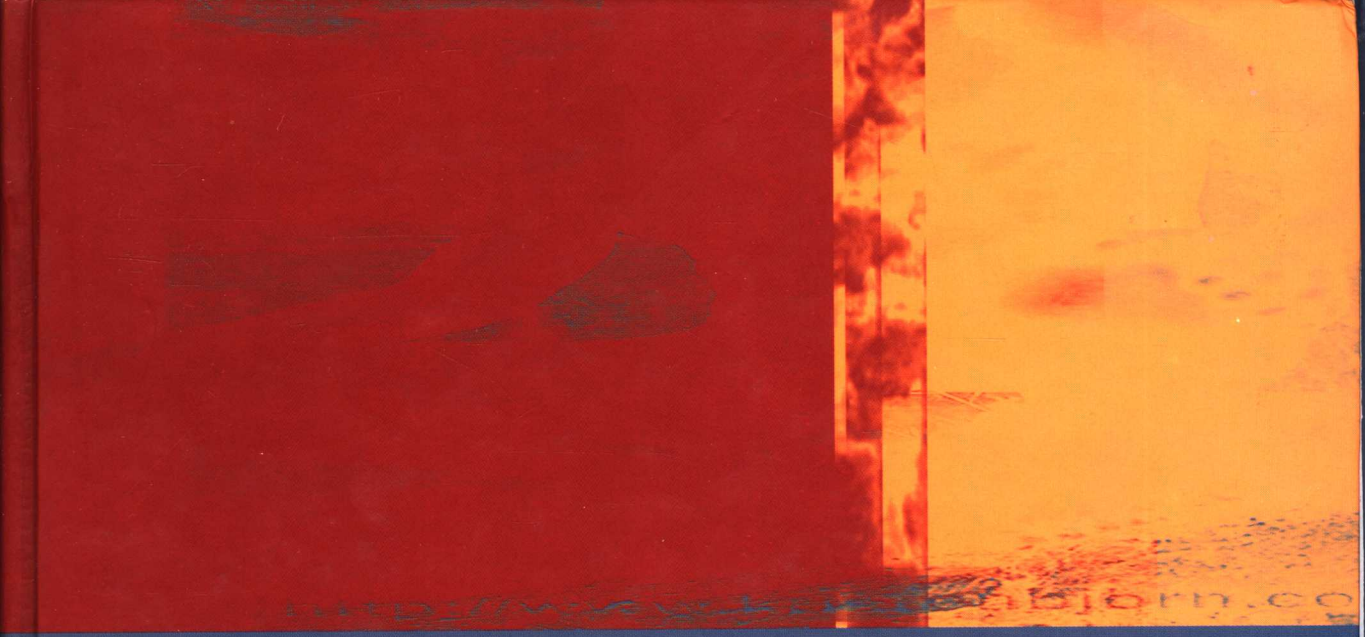

高级加密标准（AES）算法——Rijndael的设计

Joan Daemen Vincent Rijmen 著

谷大武 徐胜波 译

清华大学出版社

高级加密标准（AES）算法
——Rijndael的设计

Joan Daemen　Vincent Rijmen　著
谷大武　徐胜波　译

清华大学出版社
北 京

北京市版权局著作权合同登记号：图字 01-2002-6319 号

内 容 简 介

本书主要讲述高级加密标准（AES）算法——分组密码 Rijndael 的设计。书中全面而详尽地阐述了 Rijndael 算法的数学基础和设计原理，介绍了该算法抗击差分分析、线性分析和其他多种攻击的能力，讨论了该算法的具体实现及代码与速度的优化方法。

本书主要面向致力于密码技术和信息安全的教学、研究、设计、开发与测评的教师、研究人员、设计开发人员、测试人员、高年级本科生和研究生，是一本不可多得的参考用书。

Translation from the English language edition:
The Design of Rijndael by Joan Daemen and Vincent Rijmen
Copyright © Springer-Verlag Berlin Heidelberg 2002
Springer-Verlag is a company in the BertelsmannSpringer publishing group
All Rights Reserved.

版权所有，翻印必究。
本书封面贴有清华大学出版社激光防伪标签，无标签者不得销售。

图书在版编目（CIP）数据

高级加密标准（AES）算法——Rijndael 的设计/（比）戴尔蒙，（比）瑞蒙著；谷大武，徐胜波译. —北京：清华大学出版社，2003
书名原文：The Design of Rijindael AES: The Advanced Encryption Standard
ISBN 7-302-06305-2
Ⅰ.高… Ⅱ.①戴…②瑞…③谷…④徐… Ⅲ.密码－理论 Ⅳ.TN918.1

中国版本图书馆 CIP 数据核字（2003）第 008987 号

出 版 者：清华大学出版社（北京清华大学学研大厦，邮编 100084）
http://www.tup.tsinghua.edu.cn
责任编辑：陈仕云
印 刷 者：清华大学印刷厂
发 行 者：新华书店总店北京发行所
开　　本：787×1092 1/16　印张：16.25　字数：371 千字
版　　次：2003 年 3 月第 1 版　2003 年 3 月第 1 次印刷
书　　号：ISBN 7-302-06305-2/TP・4762
印　　数：0001～4000
定　　价：32.00 元

译 者 序

现代对称加密算法大致可分为分组加密算法和流加密算法两种。目前，在实际运行的产品和系统中，最常使用的对称加密算法是分组加密算法。从 1976 年美国数据加密标准算法（DES）公布以来，到 20 世纪末，DES 算法或其某些变形基本上主宰了对称算法的研究与开发进程。随着密码分析水平、芯片处理能力和计算技术的不断进步，专家们普遍认为，以前广泛使用的 DES 算法及其变形的安全强度已经难以适应新的安全需要，其实现速度、代码大小和跨平台性均难以继续满足新的应用需求。在这种形势下，迫切需要设计一种更强有力的算法作为新一代分组加密标准，因此 AES 应运而生。作为 AES 的候选者，国际上提出了多个分组密码算法，如 Rijndael、RC6、Twofish、Serpent、MARS 等，经过几年的专家评审、测试和反复论证，于 2000 年 10 月决定选用 Rijndael 算法作为 AES。

本书是 Rijndael 算法的设计者 Daemen 和 Rijmen 关于该算法的专著。书中全面而详尽地阐述了 Rijndael 算法的数学基础和设计原理，介绍了该算法抗击差分分析、线性分析和其他多种攻击的能力，讨论了该算法的具体实现和代码与速度的优化方法。与 DES 一样，Rijndael 算法的广泛认可和接受仍然依赖于密码研究者的进一步分析、测试与改进。因此从研究者的角度，本书有助于深入学习并理解分组加密算法的基本原理，进而提出新的算法设计和分析方法。从开发者的角度，利用本书可以更有效地写出该算法的核心代码，从而在国际竞争中争取主动。另外，由于 Rijndael 算法已经成为 AES，因此国际市场上将会陆续出现此类加密芯片，本书对于此类芯片的测试与分析也将起到促进作用。

本书是密码理论与技术方面的专著，国内尚未有如此全面地阐述 Rijndael 算法和 AES 的著作，相信本书对致力于密码技术和信息安全的教学、研究、设计、开发和测评的广大教师、研究人员、设计开发人员、测试人员、高年级本科生和研究生都是一本不可多得的参考书。

本书由 Springer 出版社授予清华大学出版社出版，清华大学出版社

对该书中译本的出版给予了大力支持，我们首先对此表示感谢。在本书的翻译过程中得到了西安电子科技大学肖国镇教授和上海交通大学白英彩教授的大力支持和鼓励，也得到了原书作者 Daemen 和 Rijmen 博士的热心帮助。同时，清华大学出版社的有关编辑同志为本书的校对和出版付出了辛勤的劳动。另外，参与本书翻译和校对工作的还有李明、曾宝珠、王弈、周蕾蕾、侯科鑫、刘含、石庆祖、温海龙等，在此一并表示衷心的感谢。

根据作者提供的勘误表，我们已经在翻译过程中对原书的一些错误做了更正；而且，还发现了原书中存在的其他错误，经与作者核对，也均进行了更正。由于我们水平有限，翻译不妥或错误之处在所难免，敬请广大读者批评指正。

译　者
上海交通大学
2002 年 10 月

试读结束：需要全本请在线购买： www.ertongbook.com

推荐序 I

20 世纪 70 年代中期由美国人开创的 DES（数据加密标准）可以说经历了近 1/4 个世纪漫长而辉煌的年代，并逐渐由繁荣走向衰落。它之所以走向衰落，是由于 20 世纪末出现了差分密码分析及线性密码分析。

美国国家标准和技术研究所（NIST）于 1997 年初发起并组织了在全世界广泛征集新的加密标准算法的活动，同时要求每一种候选算法应当支持 128、192 和 256 比特的密钥长度。经过 3 年多时间的反复较量，对首轮入选的 15 种不同算法进行了广泛的评估与测试，筛选出 5 种算法进入决赛。最终，由比利时的密码专家 Joan Daemen（Proton world International 公司）及 Vincent Rijmen（Leuven 大学）所提出的加密算法 Rijndael 幸运地赢得了胜利，成为 21 世纪新的高级加密算法 AES。

美国商业部长 Norman Minera 宣布这一最后胜利的结果时，确实出人意料，因为这是美国政府第一次将非美国公民提出的算法接受为密码标准算法，值得我们深思。

Rijndael 以其算法设计的简洁、高效、安全而令世人关注，相信它会在国际上得到广泛的应用。可喜的是，由加密算法 Rijndael 的两位创始者 Joan Daemen 与 Vincent Rijmen 合著的《高级加密标准（AES）算法——Rijndael 的设计》一书，非常系统而详尽地描述了 Rijndael 的设计思想。

谷大武与徐胜波两位博士及时而精心地翻译了本书，以期国内的广大学者有机会分享本书带给我们的优秀科学成果及卓越的设计思想。我确信，本书的翻译出版，定会引起国内广大学者的巨大反响。

自从美国科学家 Shannon 于 1949 年发表“保密系统的通信理论”从而确立了密码学的科学体系以来，经过了大约 1/4 个世纪，Rivest、Shamir 和 Adleman 创立了 RSA 公开密钥加密算法，美国国家标准局提出了 DES 体制。其后，由于差分攻击及线性攻击的出现，又经历了近 1/4 个世纪，出现了代替 DES 的新的高级加密算法——Rijndael。我想，Rijndael 也不会是永恒的，也许经过本世纪几十年的研究，会找出

Rijndael 致命的缺点，从而提出更为安全的算法。我相信，我国的年轻学者会勇敢地迎接这一挑战，担负起历史赋予信息安全的光荣使命。

肖国镇
西安电子科技大学
2002 年 10 月

推荐序 II

Rijndael 是美国新的高级加密标准（AES）征集比赛中出人意料的获胜者。美国国家标准和技术研究所（NIST）于 1997 年 1 月发起和组织了该项竞赛，并于 2000 年 10 月宣布 Rijndael 为获胜者。之所以称之为“出人意料的胜利者”，是因为许多旁观者（甚至一些参与者）对美国政府会将非美国公民设计的算法接受为密码标准持怀疑态度。

然而，不可置疑，NIST 执行了一个公开的、国际化的、可成为其他标准组织典范的选择过程。例如，NIST 的 1999 年 AES 会议在意大利罗马举行，而入围决赛的 5 个算法是由来自于世界各地的团队所设计。

Rijndael 凭借其简洁、高效、安全和原则性的设计，在最后一轮中击败了来自于 RSA、IBM、Counterpane Systems 以及一个英国/以色列/丹麦联合小组的竞争，为两位比利时设计者 Joan Daemen 和 Vincent Rijmen 赢得了最终的胜利。

书中 Rijndael 的设计者亲自讲述了算法设计的过程，概述了 Rijndael 的基础以及与作者之前设计的密码间的关系，解释了理解 Rijndael 所需的数学基础，并提供了可供参考的 C 代码以及密码测试向量。

最重要的是，本书有理由使读者相信，Rijndael 能够对抗所有已知类型的攻击。自从 1976 年 DES 被接纳为美国国家标准以来，整个领域的情况发生了极大的改变。当时，对安全性的争论主要集中在密钥的长度上（56 比特），差分和线性密码分析（我们最强有力的密码破解工具）还没有广为人知。现在，虽然已经发表了大量关于分组密码的公开文献，但一个新的算法除非它至少提供了详细的对抗差分和线性密码分析的密码强度分析，否则它不可能被接受为 AES。

本书介绍了密码设计的“宽轨迹”策略，并解释了 Rijndael 如何从该策略的应用中获益：极好的抗差分、线性密码分析性和高效率，只需要相对少的轮数就可获得强安全性。

Rijndael 被接纳为 AES 是密码学发展历史上的一个重要里程碑，它

很可能会很快成为世界上应用最广泛的密码体制。对于希望深刻理解Rijndael的人来说，由设计者自己精心撰写的这本书是“必读”的。

罗纳德L·里维斯特
计算机科学维特比教授
于麻省理工学院

前　言

本书主要讲述高级加密标准（AES）算法——分组密码 Rijndael 的设计。根据“应用密码学手册”[68]，分组密码可以描述如下：

分组密码就是一个函数，它将 n 比特明文分组映射为 n 比特密文分组，其中 n 被称为分组长度，[...]，该函数由密钥参数化。

尽管分组密码被用于许多引人注目的应用中，如电子商务和电子安全，但是本书并不打算讨论这些应用；相反，我们在书中详细描述了 Rijndael，并讲解该算法开发所依据的设计策略。

本书的结构

撰写本书时，我们主要考虑两类读者。或许大多数的读者希望本书能够给出 Rijndael 完整且准确的描述，对于他们来说，本书的第 3 章是最重要的，它对 Rijndael 进行了详尽的描述。第 2 章中的预备知识将有助于读者更好地理解第 3 章的描述，第 4 章讨论了算法的高级实现，而第 1 章则简单回顾了 AES 的选择过程。

本书余下的大部分内容则是针对那些希望了解为什么以这样的方式设计 Rijndael 的读者，包括 Rijndael 算法设计中应用的思想、原则以及宽轨迹设计策略。第 5 章讨论了 Rijndael 分组密码设计方法以及在 Rijndael 设计中扮演重要角色的准则。此设计策略源于我们的线性和差分密码分析经验，这两种密码分析攻击都曾经成功实施于此前的数据加密标准（DES）。第 6 章是对 DES 以及针对它的差分和线性攻击的简单回顾。对线性密码分析的简要描述在第 7 章，差分密码分析的描述则在第 8 章。最后，第 9 章讨论了宽轨迹设计策略是如何满足这些考虑的。

第 10 章概述了针对 Rijndael 的简化轮数变种的一些公开发表的攻击。第 11 章则给出了与 Rijndael 相关的密码的综述。我们描述这些原有的密码方案，讨论它们的相似性和区别，并对一些被 Rijndael 及其以前的算法强烈影响的密码做了简短叙述。

附录 A 说明了线性和差分分析如何能够应用于定义在有限域运算而非布尔函数上的密码算法。附录 B 讨论了差分和线性密码分析的扩展。附录 C 列出了使用一些关于 Rijndael 不同描述的表格以帮助程序员。附录 D 提供一个测试向量集合。附录 E 则包含了 Rijndael 基于 C 语言的一个范例实现。

图 1 显示了不同的阅读本书的方式。

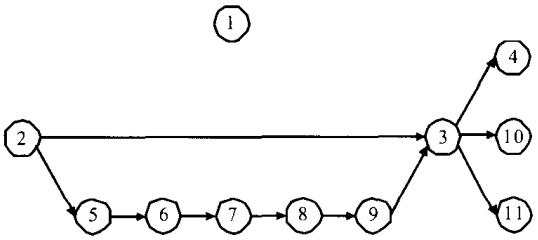

图 1 各章之间的逻辑依赖关系

本书的大部分内容已经在下列文献中公开发表：Joan 的博士论文[18]，Vincent 的博士论文[80]，我们的 AES 提案[26]，以及我们关于分组密码线性框架的论文[22]。

致谢

如果没有许多人的支持和帮助，本书是无法完成的，但在此无法将有贡献的所有人的名字一一列出。尽管如此，我们还是希望提及一些支持者的名字。

首先，要感谢那些为发展对称密码的设计理论做出贡献的密码学家，从他们那里我们学到了很多，特别是那些在设计过程初期给予我们反馈信息的人们：Johan Borst、Antoon Bosselaers、Paulo Barreto、Craig Clapp、Erik De Win、Lars R.Knudsen 和 Bart Preneel。

感谢 Elaine Barker、James Foti 和 Miles Smid 以及所有 NIST（美国国家标准与技术研究所）的工作人员，是他们的辛苦工作保证了 AES 进展的可能和可见。

感谢家人和朋友的精神支持，没有他们我们将无法坚持下来。

感谢 Brian Gladman 提供了测试向量。

感谢 Othmar Staffelbach、Elisabeth Oswald、Lee McCulloch 和其他的校对人员，是他们提供了非常有价值的反馈信息并纠正了大量的错误

试读结束：需要全本请在线购买： www.ertongbook.com

和疏忽。

最后，还要感谢提供资金支持的 K.U.Leuven、弗兰德斯科学研究基金会（比利时）、Banksys、Proton World 以及 Cryptomathic。

Joan Daemen，Vincent Rijmen

2001 年 11 月

目　录

试读结束：需要全本请在线购买：　www.ertongbook.com