信　息　安　全　系　列

国家科学技术著作出版基金
NFAPST

序列密码的设计与分析

吕述望　范修斌　周玉洁　著

北京中软电子出版社

国家科学技术学术著作出版基金资助出版

序列密码的设计与分析

The Design and Analysis on the Stream Cipher

吕述望　范修斌　周玉洁 著

北京中软电子出版社

书　　名：序列密码的设计与分析
作　　者：吕述望　范修斌　周玉洁
责任编辑：邵祖英　胡明
责任校对：凌笑
装帧设计：曾传辉
出版发行：北京中软电子出版社
地　　址：北京海淀区学院南路 55 号中软大厦 B 座 5 层
电　　话：010—62147079；51527258（传真）
电子邮件：maco856@sohu.com
经　　销：各地新华书店、软件连锁店
文本印刷：北京彩艺印刷有限公司
开本规格：787 毫米×1092 毫米　1/16 开本　11 印张　200 千字
版次印次：2003 年 1 月第一版　2003 年 1 月第一次印刷
印　　数：0001—1000 册
本 版 号：ISBN 7—900057—33—1
定　　价：68.00 元（含配套精装书、1CD)

本书的研究受到以下基金资助：

★国家重点基础研究规划（973）

（项目编号：G1999035800）

★2001 年国家高技术研究发展计划项目（863）

（项目编号：2001AA140101）

★国家自然科学基金项目

（项目编号：60173015）

★国家科学技术学术著作出版基金资助出版

内 容 提 要

本书提出了字序列密码的概念，并将其设计分为源序列发生器、非线性加工、输出合成、结合函数四部分。

第一部分源序列发生器是序列密码的驱动部分。主要讨论了上本原多项式的密度问题，初态及多项式保熵问题；环上溢出序列初态以及多项式的保熵性；M 序列作为源序列发生器时的密钥嵌入方式。第二部分，给出了四种密码学非线性加工逻辑：密码学控选逻辑、密码学迭代逻辑、密码学记忆逻辑、密码学前馈逻辑。第三部分主要以密码学相关免疫理论为基础，简单讨论了输出合成技术。第四部分，结合函数主要借鉴了分组密码设计理论与技术。给出了最大距离置换的计数公式；讨论了自逆置换集合两元素乘积的最大圈长；对 P,P^* 逻辑进行了分析。本书提出了泛函逻辑设计方法，并提出了 DP 型密码设计理念，且给出了 Fly 算法举例及分析。

本书可供从事信息安全、密码设计与分析等相关领域的研究及工作人员使用参考。

Abstract

The stream cipher includes four parts: generator of source sequences, nonlinear process, output composing, combining function.

In first part, analysis on the distributing of the primitive polynomials is given. The original state and the polynomial entropy-preservation theorems of the overflowing sequence derived from the sequence generated by the primitive polynomial on $Z/(2^e)$ are proved The methods about the keys embedded in M sequences are discussed.

In second part, the cryptographic control-choosing logic probability model is given, and sufficient condition of the mutual information between input and output being zero is gained. The cryptographic iteration logic probability model is given. The cryptographic memory with 1 bit logic probability model having two inputs is given, the outputs are independent uniform distribution sequences. The cryptographic choose-function feedforward logic probability model is given, it is proved that some methods are not the best methods to gather the information about the structure.

In the third part, the application of the cryptographic correlation-immunity theory is introduced.

In the fourth part, the concept of the maximum distance permutation is given, the counting formula is gained. Analysis of the maximum cycle length about two elements product from the set of permutation which can be inverse with itself is given. At last , P, P^* logical structures are analyzed.

总　　序

信息社会的兴起，给全球带来了信息技术飞速发展的契机；信息技术的应用，引起了人们生产方式、生活方式和思想观念的巨大变化，极大地推动着人类社会的发展和人类文明的进步，把人类带入新时代；信息系统的建立已逐渐成为社会各个领域不可或缺的基础设施；信息已成为重要的战略资源，信息化的水平已成为衡量一个国家现代化和综合国力的重要标志。争夺控制信息权已成为国际竞争的重要内容。

我国已经做出“以信息化带动工业化，发挥后发优势，实现生产力的跨越式发展”的重要决策，信息网络系统的建设和应用必将成为新世纪国家发展的重点。江泽民主席指出：“各地各部门的领导干部，必须加紧学习网络化知识，高度重视网上斗争的问题。我们的党建工作、思想政治工作、组织工作、宣传工作、群众工作，都应适应信息网络化的特点，否则是很难做好的。总之，对信息网络化问题，我们的基本方针是积极发展，加强管理，趋利避害，为我所用，努力在全球信息网络化的发展中占据主动地位。”

然而，人们在享受信息网络所带来的巨大利益的同时，也面临着信息安全问题的严峻考验。现存的信息安全问题已经对我国的国家安全、经济安全、军事安全和社会安全构成了严重的影响和威胁，我们面临着信息安全的巨大挑战。国家“十·五”国民经济发展计划决定了要“强化信息网络的安全保障体系”。因此，加速信息安全的研究和发展，加强信息安全保障能力已成为我国信息化发展的当务之急，成为国民经济各领域电子化成败的关键，成为提高中华民族生存能力的头等大事。为了构筑二十一世纪

的国家信息安全保障体系，有效地保障国家安全、社会稳定和经济发展，需要尽快地并长期致力于增强广大公众的信息安全意识，提升信息系统研究、开发、生产、使用、维护、教育管理人员的素质和能力。

当今，信息安全的概念正在与时俱进：它从早期的通信保密发展到关注信息的保密、完整、可用、可控和不可否认的信息安全，并进一步发展到现今的信息保障和信息保障体系。单纯的保密与静态的保护已都不能适应今天的需要。信息保障体系是一个社会系统工程，它不仅涉及到信息技术体系本身还包括有信息安全的法律法规体系和组织管理体系。因此，现阶段以及未来的有效信息安全整体解决方案应依赖于人利用技术进行操作这三个层面。而实施完整的信息保障战略还必须依赖于人才的培养和经费的支持。

中软电子出版社为适应上述形势的需要，经与国家信息安全领导机关和管理部门、信息安全的学术团体和研究机构、信息安全主要使用单位和行业、国内外知名专家进行了大量的请示、商榷和研究，决定成立《信息安全系列》丛书编委会。《信息安全系列》丛书编委会由上述有关专家和部门主管领导组成，目前已聘请到信息安全领域的两院院士 4 位、政府有关主管部门的领导 7 位、博士生导师 12 位。它在国家信息化领导小组的宏观政策指导下，通过长期的努力，组织出版和发行这套丛书。丛书的指导思想是求新、求精、求快、求用，要围绕国内外信息安全的新技术、新发展、新知识和我国市场需求的原则进行考虑；丛书的选题范围是根据读者群定位为通俗、教育培训、领导和专业等四个层次；丛书的内容涉及信息安全技术、信息安全法律法规和信息安全管理等三个类型六个方面。由编委会确定《信息安全系列》丛书的组织结构、选题、作者、编著时间等方案；发挥编委会成员的影响力，把正在或将要编写的符合本丛书出版原则的书稿作者汇聚在编委会的周围，形成我国最有权威、最有影响力的《信息安全系列》丛书编委会。为普及、提高、推广和发展信息安全理论和技术做出我们应有的贡献。

编委会设主任 1 人（沈昌祥院士）；副主任 2 人（赵战生博导、吕述望博导）；编委会下设秘书处（秘书长邵祖英教授、副秘书长高伟红副教授等若干人）、编辑部（主任曾传辉博士、副主任吴东副编审等若干人）、写作室 6 个。考虑到在运作推出《信息安全系列》丛书过程中的复杂性、艰巨性、长期性，因此，必须花大力气依靠编委会全体成员，用若干年的时间，完成这项宏大工程。

沈昌祥

2002 年 3 月 18 日

前　言

关于序列密码设计，已有若干理论研究成果。本书在总结已有序列密码设计与理论的基础上，在具体的序列密码的设计实践中，进一步提出了字序列密码的概念，并将字序列密码的设计分为源序列发生器、非线性加工、输出合成、结合函数四部分。

第一部分主要包括第一、二、三章。源序列发生器是序列密码的驱动部分，一般情况之下，其目的是产生长周期的伪随机序列。由于 m, M 序列、环导出序列的研究已比较完备，本部分仅就我们在具体序列密码设计中的几个关心问题做了讨论。第一章主要讨论了 F_2 上本原多项式的密度问题，初态及多项式保熵问题；第二章主要讨论了环上溢出序列初态以及多项式的保熵性；第三章讨论了 M 序列作为源序列发生器时的密钥嵌入方式。

一般情况之下，由于源序列发生器带有明显的线性或代数特征，所以在序列密码的设计之中，要对其进行非线性加工。作为序列密码设计的第二部分，我们主要利用概率论、信息论、随机过程等工具，对其进行了理论研究和分析。我们归纳出主要的四种密码学非线性加工逻辑：密码学控选逻辑、密码学迭代逻辑、密码学记忆逻辑、密码学前馈逻辑；并将其研究结果分别列入第四、五、六、七章中。

为抵抗非线性加工的分别攻击方法，我们给出了序列密码设计中的第三部分：输出合成。第九章中，我们主要以密码学相关免疫理论为基础，简单讨论了输出合成技术。

第四部分中，结合函数主要借鉴了分组密码设计理论与技术。第九章给出了最大距离置换的计数公式；第十章讨论了自逆置换集合两元素乘积的最大圈长；第十一、二章主要利用概率论与随机过程论给出了 *Fly* 算法

中的 P 逻辑的线性与差分分析，P^* 逻辑的线性与差分基本分析。

本书是作者在序列密码的具体设计实践中所遇问题的研究结果，所以本书属应用基础研究。

继布线逻辑设计，存储逻辑设计，运算逻辑设计之后，本书中，进一步提出了泛函逻辑设计方法。泛函逻辑设计方法将在今后的密码设计实践中发挥重要作用。本书还提出了 DP 型密码设计理念，并给出了 Fly 算法举例及分析。

借此，对中国科学院信息安全国家重点实验室刘振华教授、赵战生教授、裴定一教授、冯登国教授、叶顶峰教授等各位老师的指导与帮助表示衷心感谢！

对蔡吉人院士、周仲义院士、魏正耀院士、陈华平研究员、黄民强研究员、李世取教授、郑建华研究员、韩文报教授、张宝东研究员、戚文峰教授等各位专家的指导与帮助表示衷心感谢！

对北京中软电子出版社的各位老师的热情帮助与支持表示衷心感谢！

对各位同学与同事的热情帮助与支持表示衷心感谢！

本书是在范修斌博士的中国科学院研究生院博士后研究工作报告基础上写成的。对宋广娟女士的书稿输入以及对若干数学公式的演算所付出的劳动表示衷心的感谢！

由于作者水平所限，不足之处，欢迎专家与读者指正！

作　者

2002 年 10 月 1 日于北京

目　　录

第三部分 输出合成

第四部分 结合函数

绪　论

关于序列密码设计，已有若干理论研究成果。本书在总结已有序列密码设计与理论的基础上，在具体的序列密码的设计实践中，进一步提出了字序列密码的概念。所谓字序列密码是指含有以字为运算单元的序列密码。书中将字序列密码的设计分为源序列发生器、非线性加工、输出合成、结合函数四部分。

源序列发生器是序列密码设计的第一部分，是序列密码的驱动部分，是古典序列密码中轮子或圆盘的继承与发展。近现代数学理论在序列密码源序列发生器设计中的引入与发展，使序列密码的设计由艺术发展为科学技术。

源序列发生器目前比较成熟的研究结果主要包括：二元线性递归序列；环导出序列；M 序列。源序列发生器的主要功能是产生长周期的伪随机序列，借以驱动序列密码的非线性加工部分，输出合成部分，结合函数部分。显然源序列发生器部分具有明显的线性或代数特征，序列密码的其余三部分正是对此的进一步数

学处理。

以有限域，环论，线性移位寄存器，自动机，离散傅立叶变换(*Walsh* 谱)分析，数论等数学理论为工具，对二元线性递归序列的密码学性质的研究已比较完备。结合现在密码学中的概念及应用，在第一章中，我们进一步给出了如下结果：m 序列初态保熵，多项式保熵，从而讨论了密钥更换的有效性；本原多项式的密度分析；m 序列产生的置换为正形置换，从而指出了序列密码设计的基础乱源与分组密码设计的基础置换的内在联系。

环论，*Galois* 环，*Chrestenson* 谱，L^3－算法，*Gröbner* 基理论，域论，数论等是研究环上序列密码学性质的主要数学工具。虽然二元线性递归序列具有较好的伪随机特性，但其线性复杂度较小，难以对抗攻击，比如 BM 算法，解线性方程组等攻击算法。人们发现剩余类环上存在极大长线性递归序列，并且其最高权位序列可作为环导出二元序列，具有较好的伪随机特性以及足够大的线性复杂度。在序列密码的设计中，环导出二元序列作为源序列发生器，体现了环上运算域上用的特点。值得指出的是我国学者曾肯成、戴宗铎、黄民强、戚文峰等在环导出序列的研究成果突出，在国际上有一定的地位。其中，第一、三保熵定理是关于初态作为密钥更换有效性的研究，但易知同圈平移等价。第二保熵定理是关于多项式作为密钥更换有效性的研究，且更换时非平移等价，为我们密码设计提供了更好的理论基础。鉴于环上极大长序列工程实现中，其溢出序列比较容易得到，那么溢出序列是否具有良好的密码学特性？能否作为密码学资源？本书第二章给出了溢出序列初态以及多项式保熵性证明。

图论，非线性移位寄存器，布尔函数论，m值逻辑函数论，环上序列论等是M序列密码学性质研究的主要数学工具。但目前M序列的生成速度制约了其在密码设计中的广泛应用。本书第三章仅讨论了M序列作为源序列发生器的密钥嵌入方式。

一般情况之下，由于源序列发生器带有明显的线性或代数特征，所以在序列密码的设计之中，要对其进行非线性加工。作为序列密码设计的第二部分，我们主要利用概率论、信息论、随机过程论等数学工具，对其进行了理论研究和分析。我们归纳出主要四种密码学非线性加工逻辑：密码学控选逻辑、密码学迭代逻辑、密码学记忆逻辑、密码学前馈逻辑；并将其研究结果分别列入第四、五、六、七章中。

域论，环论，概率论，测度论，随机过程，鞅论，数理统计，贝叶斯估计理论，信息论等是研究密码学控选逻辑的主要数学工具。已有研究结果主要包括：钟控序列的线性复杂度分析；钟控序列的周期分析；钟控序列的攻击方法。在几种常见的密码学控选逻辑技术的基础上，第四章给出了一般密码学控选逻辑的概率模型，得到了密码学控选逻辑控制序列与输出序列互信息为零的一个充分条件。众所周知，剩余类环上的本原多项式输出序列低权位信息的抗攻击能力较弱。若利用剩余类环上的本原多项式为源序列发生器，利用密码学控选逻辑序列概率模型进行非线性加工,当控制序列与输出序列互信息为零时，则可利用源序列发生器输出序列的低权位信息作为控制序列，从而可以较为充分的利用剩余类环上的本原多项式的输出序列这一密码学资源。所以本章的研究结果对于密码编码学中的环上序列密码的设计，有着一定的意义。本章最后，首次利用信息论的方法，讨论了[1，3]型钟

控序列的钟控输入序列与输出序列的互信息；证明了互信息是输出序列长度的严格单调增函数，并且给出了互信息的发散速度；证明了钟控输入输出互信息大于输出序列单点独立提供的信息量之和。

随机过程、信息论等是研究密码学迭代逻辑的主要数学工具。在密码编码学中，人们经常利用密码学函数迭代技术来实现密码算法，例如 DES、RC4、RC5、AES、序列密码的非线性加工部分等，其所依赖的理论基础包括相关免疫理论，扩散准则，雪崩原理等。众所周知，信息论原理是密码编码学以及密码分析学的重要理论组成部分。第五章的出发点是利用信息论原理对密码学函数迭代技术建立信道迭代模型。在此基础上，进一步利用随机过程理论，给出密码学函数迭代原理分析，得到了经过密码学函数迭代之后输出为均匀分布时，输入输出互信息极限为零的充分必要条件，以及在一定条件之下的输入输出互信息收敛速度的一个上界。

1984 年，*Rueppel* 提出了带记忆的非线性组合器，为进一步考察其密码学性质，第六章给出了 1 比特加法记忆独立二输入逻辑的概率模型，证明了其输出序列是独立均匀同分布的二元随机变量序列，并给出了其信息论分析结果。

域论，概率论，数理统计，贝叶斯估计理论，信息论，密码学相关免疫理论，密码学谱论等是研究密码学前馈逻辑的主要数学工具。已有的主要研究结果：前馈序列的线性复杂度，极小多项式；前馈序列的统计特性等。前馈序列具有良好的伪随机特性，线性复杂度较大，统计特性良好，其作为非线性加工技术，在序列密码的设计之中得到了广泛的应用。第七章主要以简单选择函数前馈逻辑为例，提出了联合分布全息采集方法的概念，并给出