流密码学及其应用

丁存生　肖国镇　著

国防工业出版社

流密码学及其应用

丁存生 肖国镇 著

国防工业出版社

(京)新登字106号

图书在版编目(CIP)数据

流密码学及其应用/丁存生,肖国镇著.—北京:国防工业出版社,1994

ISBN 7-118-01258-0

Ⅰ.流… Ⅱ.①丁… ②肖… Ⅲ.①流密码学②流密码学-应用 Ⅳ.TN918.1

流密码学及其应用

丁存生 肖国镇 著

责任编辑 马征宇

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 100044)

新华书店经售

北京市王史山胶印厂印刷

*

开本 850×1168 1/32 印张 9⅛ 231千字

1994年9月第1版 1994年9月北京第1次印刷 印数 1—16 000册

ISBN 7-118-01258-0/TN·198 定价:12.10元

(本书如有印装错误,我社负责调换)

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，国防科工委于 1988 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. 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，对国防科技发展具有较大推动作用的专著；密切结合科技现代化和国防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，密切结合科技现代化和国防现代化需要的新工艺、新材料内容的科技图书。

4. 填补目前我国科技领域空白的薄弱学科的边缘学科的科技图书。

5. 特别有价值的科技论文集、译著等。

国防科技图书出版基金评审委员会在国防科工委的领导下开展工作，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，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，是对出版工业的一项改革。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工业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

第二届评审委员会组成人员

名誉主任委员	怀国模			
主任委员	黄　宁			
副主任委员	殷鹤龄	高景德	陈芳允	曾　铎
秘书长	刘琯德			
委员 (按姓氏笔划为序)	尤子平	朱森元	朵英贤	
	刘　仁	何庆芝	何国伟	
	何新贵	宋家树	张汝果	
	范学虹	胡万忱	柯有安	
	侯　迁	侯正明	莫梧生	
	崔尔杰			

前　言

密码技术用于保护军事和外交通信可追溯到几千年前。在今天的信息时代，大量的敏感信息如病历、法庭记录、资金转移、私人财产等常常通过公共通信设施或计算机网来进行交换，而这些信息的秘密性和真实性是人们迫切需要的。因此，当代密码学的应用已不再限于军事、政治和外交，其商用价值和社会价值已得到了充分肯定。

密码学包含密码编码学和密码分析学两个分支。前者寻求保证消息保密性或真实性的方法，而后者则研究加密消息的破译或消息的伪造。

密码学的历史可大致划分为以下几个阶段：从古代到 1949 年可看作是科学密码学的前夜时期，该时期的密码技术可以说是一种艺术，而不是一种科学。那时密码专家常常是凭直觉和信念来进行密码设计和分析，而不是靠推理证明。1949 年单农(Shannon)发表的《保密系统的信息理论》一文为单钥密码系统建立了理论基础，从此密码成为一门科学，但从 1949 年到 1975 年这段时期密码学理论的研究工作进展不大。1976 年狄非(Diffe)和海尔曼(Hellman)的《密码编码学新方向》一文导致了密码学上的一场革命。他们首次证明了在发端和收端无密钥传输的保密通信是可能的，从而开创了公钥密码学的新纪元。

公钥密码学是密钥分配问题和消息认证问题的产物。许多公钥系统既可用于认证，又可用于消息保密。近年来，人们已认识到了认证和保密是两个独立的密码属性。西蒙恩(Simmons)对认证问题进行了系统的研究，他建立了一套与单农保密理论平行的认

证理论。

密码按加密形式可分为流密码和分组密码，前者又称为序列密码。近年来，流密码的理论得到了长足的发展。相对而言，分组密码的研究进展较慢。其主要原因有以下几点：其一，前者中的同步密码结构较后者简单；其二，前者有较为理想的数学分析工具，如频谱理论和技术、代数等；其三，分组密码的一个不足之处在于相同的明文组对应相同的密文组，这给密码分析者充分利用明文语言的多余度提供了可能性。这就是说，密文的串检验破译对分组密码是一种挑战；其四，目前大多数国家的军事和外交保密通信似乎仍主要使用流加密方式。

自从密码技术及其理论诞生以来，密码系统的强度问题一直在困扰着密码设计者和分析者，问题的关键在于强度度量指标问题。传统分组密码和公钥密码的强度研究目前无多少进展，但流密码系统强度问题的研究已取得了突破性进展。

60 年代末提出的线性反馈移位寄存器 B-M 综合算法使得线性复杂度成为一些流密码系统强度的重要指标。从此，各种流密钥序列的线性复杂度分析取得了丰硕成果。但直到 80 年代中期，流密码学的研究仅限于一些相关方法的探讨和线性复杂度分析。80 年代末期，重量复杂度、球体复杂度、变复杂度距离、定复杂度距离、球面周期、球体周期、函数稳定性和信源码稳定性指标的引入及各种指标之间关系的建立，产生了流密码稳定性这一新理论，使得流密码的强度问题研究得到了重大突破。这一新领域的探讨将对公钥密码系统和传统分组密码稳定性的研究起到积极的推动作用。

国内目前已有几本密码学著作，但这些著作涉及流密码的内容很少。国外专门论述流密码的有两本著作：一本是司根塔勒(Siegenthaler)的博士论文《流密码系统的设计方案》，另一本是卢珀(Rueppel)的研究专著《流密码的分析与设计》。前者主要讨论流密码的相关分析，后者着重分析流密钥序列的线性复杂度。由于流密码理论近年来发展较快，这两本著作已不能反映流密码学的研

究现状。鉴于流密码的分析和设计在军事和外交保密通信中有重要应用价值，而国内目前尚无专门论述流密码学的著作，本书将我们与单炜娟同志初步建立的“流密码稳定性理论”与国内外散见于各种刊物上的文献结合起来并给予系统化，力图反映当代流密码学的主要领域和研究现状。我们期望这本书对我国保密通信的应用研究和理论研究工作者有所促进。

本书以介绍我们在流密码稳定性理论方面和流密码的频谱分析方面所做的研究工作为主，这些工作属国家自然科学基金和军事电子科研基金资助的几个研究项目。全书共十二章，含 71 节和四个附录，其中 39 节和两个附录介绍了本书作者与单炜娟的研究工作。

本书对流密码学中的某些错误研究趋势进行了分析与论证，对目前的一些新研究方向提出了质疑(例如，二次复杂度问题等)。此外，本书对我们的观点和其他学者的观点进行了区分，并在每章最后附加一个注记，其目的是进一步说明本章问题的研究现状，同时尽可能说明每章节中每个定理和引理的来源。

在介绍文献成果的同时，我们注重对各种密码思想和方法的提炼。为使读者进一步了解流密码的研究现状，我们在书中提出了 20 个研究问题，并在附录四中列出了研究问题目录，以便于关心研究工作的读者查阅。

本书第一章介绍了保密系统的信息理论和流密码系统分类。鉴于频谱理论和技术是流密码相关分析和稳定性分析的一个重要工具，我们在第二章以很小的篇幅介绍了频谱方面的基础知识。第三章系统地介绍了密钥流序列的基础理论，这章对序列的分析是从密码学角度出发的。第四章给出了密钥流序列稳定性理论的基本框架，各种具体密钥流序列的稳定性讨论将在相应的章节中进行。第五、六、八、九章对四大类流密码系统的攻击方法和稳定性等进行了探讨。作为应用，§6.5 讨论了线性复杂度及其稳定性在抗干扰扩频通信中的应用，其目的是促进这两个研究领域的沟通。第七章对相关免疫函数及其密码学价值进行了系统分析。第十章研

究对称函数的稳定性，属流密码稳定性理论的一个组成部分。第十一章着重讨论 M 序列的密码特性。第十二章对流密码中的一些专题进行了讨论。由于算法在密码学中的重要性，本书的三个附录介绍了三种计算序列线性复杂度的算法。

作为一本起点高且覆盖流密码学各个主要研究方向的专著，本书没有专门的章节介绍书中所需的数学知识和密码学基础知识。有关有限域、算法与问题复杂度、编码理论和扩频通信方面的内容可参考其他著作。

作者对胡国定教授、王新梅教授、王育民教授和刘向武研究员给予的支持深表谢意。单炜娟同志对本书的撰写提出了许多宝贵意见，并在本书的修改方面做了许多工作，在此特表谢意。作者还感谢冯登国、任朝荣、陈爽三位研究生及李长虹同志在本书抄写方面所做的工作。特别是冯登国同志花了大量时间审定原稿，修改了原稿中多处疏漏，简化并改正了某些定理的证明。

国家自然科学基金会、军事电子预研基金会、国家保密通信研究基金会和西安电子科技大学对作者所从事的几个密码学研究项目给予了大力支持，在此表示谢意。

最后，我们在此特别感谢国防科技图书出版基金评审委员会的专家教授，本书的出版与他们的大力支持是分不开的。

应看到，我们初步建立的流密码稳定性理论还不完善，有许多问题还需进一步探讨。作者恳切期望得到读者们的批评和指正。

作　　者

1992 年 5 月 20 日

目　录

第一章　流密码体制

§1.1　保密系统的 Shannon 模型

在通信系统和保密系统之间有一种对偶关系。在信道有干扰的情况下，通信系统设计者寻求使得消息在消息宿（信宿）无误地恢复。既使信道无噪声，保密系统设计者也试图使得局外人难以复原消息。单农（Shannon）在 1948 年发表了题为《通信的数学理论》后，于 1949 年又推出了与此相关的经典著作《保密系统的信息理论》。该文建立了单钥保密系统的理论基础且多年来对保密系统的设计具有指导意义。图 1.1 为保密系统的单农模型。M 元组 $X=(x_1,\cdots,x_M)$ 为消息或明文，通常假定 x_i 为二元数字。N 元组 $Y=(y_1,\cdots,y_N)$ 是在不安全信道上传送的密文，也就是说，敌方密码分析者可以得到这些密文。K 元组 $Z=(z_1,\cdots,z_K)$ 是通过安全信道传送到信宿的密钥，这就是说，敌方密码分析者无法得到该密钥。

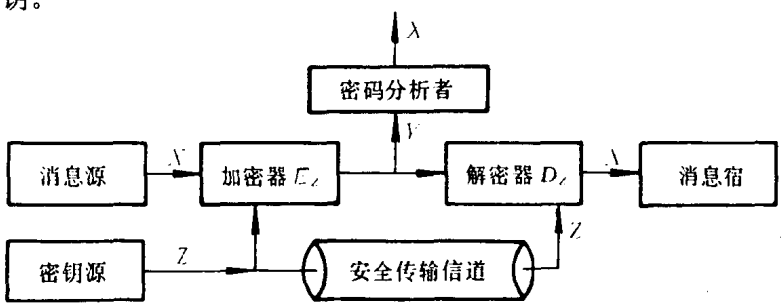

图 1.1　保密系统的单农模型

密钥 Z 确定一个特殊的置乱算法，使得加密器作用到明文上产生密文。换言之，加密器实现一个由 Z 的值所确定的特殊函数 $E_Z(\cdot)$，其运算可表示为

$$Y = E_Z(X) \tag{1.1.1}$$

显然，Y 是 X 和 Z 的一个函数，但我们将式(1.1.1)的右端写成 $E_Z(X)$ 而不是 $E(X,Z)$，其目的是为了强调密钥的选择确定一个 X 和 Y 之间的函数关系。

解密器的任务是用密文和密钥恢复明文，它实现一个函数 $D_Z(\cdot)$，使得

$$X = D_Z(Y) \tag{1.1.2}$$

或等价地，使得对每个可能的密钥 Z 和所有可能的明文 X 有

$$X = D_Z[E_Z(X)] \tag{1.1.3}$$

在密码编码学中，人们习惯上假定密码分析者拥有加密器和解密器。这样，密文的秘密性仅依赖于密钥。在实践中，同一密钥用来加密几段明文。例如，每周更换一次密钥。通常将对一个保密系统的攻击分为以下几种：

(1) 唯密文攻击：密码分析者有一个或更多的用同一密钥加密的密文。

(2) 已知明文攻击：除待解的密文外，密码分析者有一些明文和用同一密钥加密这些明文所对应的密文。

(3) 选择明文攻击：密码分析者可得到所需要的任何明文所对应的密文，这些密文与待解的密文是用同一密钥加密得来的。

保密系统设计者当然期望该系统能抵抗选择明文攻击。如果做不到的话，他希望该系统能抵抗已知明文攻击。至少他希望该系统能抵抗唯密文攻击。

一般而言，对任何密码，当一个密码分析者能够很快地从密文确定出明文时，他将认为自己已经破解了该系统。这通常意味着他能够快速地找到所使用的密钥。对于相当一部分密文，如果他可以很快从密文确定出明文或者一大段明文的话，他仍然认为该系统已被破解。没有严格的准则来说明何时一个密码系统被破解。

§1.2 基于信息理论的保密系统分析

我们现在对图 1.1 所描述的保密系统的单农模型进行数学分析。前面我们已经提到过，在实际系统中一个密钥被用来进行多次加密。为了简化描述用一个密钥进行多次加密的概念，我们假定图 1.1 中的明文 X 是用同一方法编码后的所有明文的并列。因此，在本节我们假设在图 1.1 的保密系统中，每次加密后密钥都变化。

关系式(1.1.2) 告诉我们，Y 和 Z 一起唯一地确定 X。由此得出，式(1.1.2) 等价于

$$H(X|YZ) = 0 \tag{1.2.1}$$

上述关系式(1.2.1) 是很明显的。为了得到一个较为复杂的关系，我们首先引入一个定义。如果

$$I(X;Y) = 0 \tag{1.2.2}$$

则我们说一个保密系统是完善的。由于式(1.2.2) 意味着 X 和 Y 是统计独立的，故上述定义是合理的。在这种情况下，密码分析者从 Y 来估计 X 与从任何一个随机选取的可能密文来估计 X 无任何区别。但需要强调的是，我们这里所谈的安全性是对唯密文攻击而言的。一个完善保密系统在已知明文攻击下可能是极为不安全的。完善保密系统是否存在并不是很明显的。在回答这个问题之前，我们先证明下面的结果。

定理 1.2.1 在一个完善保密系统中

$$H(Z) \geqslant H(X) \tag{1.2.3}$$

证明 由式(1.2.2) 得到

$$\begin{aligned} H(X) &= H(X|Y) + I(X;Y) \\ &= H(X|Y) \end{aligned} \tag{1.2.4}$$

再由式(1.2.1) 得知

$$\begin{aligned} H(X|Y) &\leqslant H(XZ|Y) \\ &= H(Z|Y) + H(X|YZ) \\ &= H(Z|Y) \end{aligned}$$