密码学与语音保密通信

吴伯修 曹秀英

东南大学出版社

密码学与语音保密通信

吴伯修　曹秀英

东南大学出版社

内 容 提 要

本书重点讨论密码学与语音保密通信。主要内容包括：密码学的数学基础知识和编码的基本知识、语音信号处理、公钥密码导论、保密通信、自适应回波抵消技术、有线信道自适应均衡及一种异步话音置乱体制研究。

本书可作为高校无线电通信专业研究生的教材或参考书，也可供研究保密通信方面的科技人员参考。

责任编辑：李　玉　张　克
责任校对：陈阿明　张　克
责任印制：陈　跃

密码学与语音保密通信

吴伯修　曹秀英

*

东南大学出版社出版发行
（南京四牌楼2号　邮编210018）
江苏省新华书店经销　南京邮电学院印刷厂印刷

*

开本850×1168毫米 1/32　印张16.5　字数425千
1996年12月第1版　1996年12月第1次印刷
印数：1—800册
ISBN　7—81050—114—3/TN·12
定价：28.00元
（凡因印装质量问题，可直接向承印厂调换）

此为试读，需要完整PDF请访问：www.ertongbook.com

前　言

密码学与语音保密通信自它产生的那一天起，就带有浓厚的神秘色彩，并主要为与军事、政治、外交、安全有关的保密机关所掌握。Shannon 在 1949 年发表了“保密通信的信息理论”一文，将保密学、密码学的研究引入了科学的轨道。但当时并未引起科学界和工程界的强烈反响，直到 30 年后的 70 年代，随着信息时代的到来，才引起了人们的重视。步入 90 年代的今天，信息的传输、变换、压缩、存贮等信息处理的实时性、可靠性和安全性，已成为人们迫切要求解决的问题。

本书是作者根据多年指导研究生及从事科学研究的实践，并在参考了国内外大量有关文献资料的基础上，编写而成。

吴伯修教授早在 1993 年就为本书拟定了详细的编写大纲，并着手整理撰写，但不幸因突发心脏病而离开了人间，遗憾的是，我们仅找到他的亲笔遗稿三章。为了完成吴伯修教授的生前遗愿，除对该三章进行了必要整理作为本书的第 1、2、3 章外，还将吴伯修教授已出版图书中的有关内容摘录，作为本书的第 5 章；其他章节由第二

作者书写而成。

本书分密码学、语音保密通信两大部分。在密码学部分主要介绍了密码通信的数学基础、编码基本知识、语音信号处理、公钥密码导论；在语音保密通信部分主要介绍了保密通信、自适应回波抵消技术、有线信道自适应均衡、异步语音置乱体制。保密通信是作者多年指导研究生和从事科学研究成果的结晶，尤其无需帧同步的模数模保密机，是不同于同步保密机的一种新体制。从1985年起至今，在此领域中的研究不断深入，全双工保密通信中的两大难题：有线信道的自适应均衡和自适应回波抵消，无论从理论上还是从实践上都很好地得到了解决。

由于时间仓促，书中错误之处在所难免，诚请读者批评指正。

编者

1996.10

目　　录

第1章　绪　论…… 1
1.1　引　言 …… 1
1.2　消息的加密和传输 …… 3
1.3　保密通信、信息论、密码学之间的关系 …… 5
第2章　密码通信的数学基础…… 8
2.1　引　言 …… 8
2.2　数论的基本知识 …… 8
2.3　密码学的代数基础…… 28
2.4　密码学的基本知识和术语…… 72
第3章　编码的基本知识 …… 74
3.1　二进制编码…… 74
3.2　编码的基本知识…… 78
3.3　有关的其他码…… 88
第4章　公钥密码导论…… 100
4.1　引　言 …… 100
4.2　指数加密算法 …… 101
4.3　RSA 公钥系统 …… 105
4.4　Rabin 方法及其安全性证明 …… 108
4.5　素数概率检验法 …… 111

4.6 背包公钥系统 …… 113
4.7 背包公钥的若干补充 …… 120
4.8 其他公钥系统 …… 120
4.9 鉴别和签名 …… 121
4.10 应用举例 …… 123
4.11 传统密码的签名 …… 127
4.12 概率加密 …… 129
4.13 对低密度背包系统的破译方法 …… 137
第5章 保密通信 …… 144
5.1 引 言 …… 144
5.2 保密通信系统的数学模型 …… 144
5.3 密码体制的基础知识 …… 146
5.4 完全保密系统 …… 156
5.5 熵和疑义度 …… 159
5.6 随机密码 …… 165
5.7 实际保密系统 …… 169
5.8 话音保密系统 …… 171
5.9 扩展频谱通信 …… 191
第6章 语音信号的处理 …… 195
6.1 引 言 …… 195
6.2 移位寄存器序列及伪随机码 …… 196
6.3 短时富里叶变换 …… 204
6.4 语言保密体制 …… 238
6.5 语音处理的时域方法 …… 263
第7章 自适应回波抵消技术 …… 307

此为试读,需要完整PDF请访问: www.ertongbook.com

7.1 引 言 …… 307
7.2 变步长的抗干扰稳健自适应滤波算法 …… 313
7.3 基于正交原理的干扰检测算法 …… 325
7.4 主输入端加自适应预测预处理的自适应滤波器 …… 334
7.5 基于 MMKE 准则的自适应格形梯度算法 …… 342
7.6 自适应回波抵消技术在全双工模拟语音置乱系统中的应用 …… 351
7.7 改进后的 LMS 自适应滤波算法 …… 378
第 8 章 有线信道的自适应均衡 …… 385
8.1 引 言 …… 385
8.2 信道加性白噪声对 LMS 算法性能的影响 …… 387
8.3 信道估算均衡 …… 394
8.4 计算机模拟 …… 409
8.5 有线信道自适应均衡器的实现 …… 418
8.6 测试及结果分析 …… 426
第 9 章 异步语音置乱体制 …… 435
9.1 引 言 …… 435
9.2 异步语音置乱 …… 435
9.3 语音置乱的实质和异步工作的原理 …… 453
9.4 异步语音置乱的抗密码分析能力 …… 465
9.5 异步语音置乱方案的实现 …… 476
9.6 异步语音加密装置的性能分析 …… 495
参考文献 …… 515

第1章 绪 论

1.1 引 言

保密通信是对欲传输的消息采取加密措施后才在信道中传送，而收端则对所收到的加密消息进行解密（即加密措施的逆操作）使它恢复原消息的一种通信方式。加密的目的是隐蔽消息内容，使窃听者或无关人员在收到加密消息后无法获得原消息，而收方则可用预先约定的密钥（解密方法）方便地把收到的加密消息无错误地变换为原消息。

早在中世纪，罗马皇帝凯撒就已经在高卢战争中使用单代替密表，后来发展为如图 1.1 所示的轮盘式密码装置。这种装置是由两个同轴的轮盘组成，外轮盘可以自由转动，使写在外轮盘上的英文字母与写在内轮盘上的小写英文字母一一对应。例如，图示中 A 和 x，E 和 b，……等相对应。若把外轮盘上的大写字母作为原消息（明文）字母，内轮盘上的小写字母作为加密消息（密文）字母，则该图的 26 个对应关系就是凯撒所用的单代替密表。若把外轮盘再旋转 $(360/26)^\circ$ 角度时，就可得到另一种两组字母间的对应关系，这就相当于更换了一张单代替密表。用密码学的术语，这种用轮盘式密码装置得到的是属于简单代替的加密方法。

长久以来保密通信的知识和手段主要掌握在与军事、政治、外交有关的保密单位手中。直到 70 年代，由于通信的手段日臻完善，信息传输日益迅速，导致人们对商业情报、计算机程序，甚至个人私事，越来越迫切需要保密通信。另一方面，由于科学技术的发展，人们已经能够生产体积小、重量轻、价钱便宜且保密度高的加、解

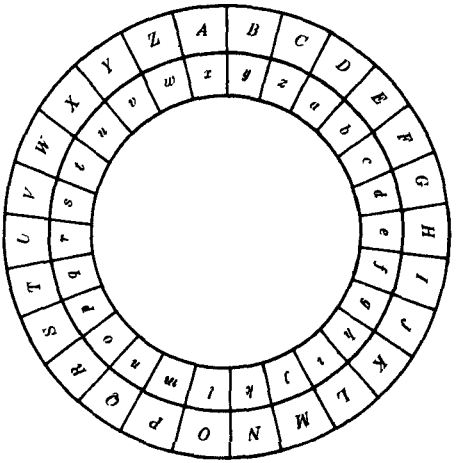

图 1.1　轮盘式密码装置

密装置，从而大大地扩大了保密通信的应用范围，导致了密码学知识在民间的传播。在高等学校中也开始出现了一批不属于保密单位的密码学及其技术的研究人员。他们可以不受限制地发表论文，相互切磋、相互竞争，从而加速了密码学及其技术的发展。目前，密码学及其有关技术已经得到数学、信息、计算机科学、通信工程等方面的学者的广泛关注。

本书的重点在于介绍现代语音保密通信技术、现代密码学的基础知识。扩展频谱通信除了有一定保密性外，由于它在信道中传输时的功率谱强度往往远低于信道中的干扰，因此采用这种通信体制来传送加密消息可提高其抗截获能力。故本书也有专章介绍扩频技术在保密通信中的应用。目前，语音加密装置有数字加密和模拟加密两大类。数字加密有较好的保密性能，但需要使用较宽频带的信道来传送。对于窄带信道，一般要与声码器联合使用，先压缩数字话音的数码率，然后再进行数字加密，使它能够通过窄带信道(例如语音信道)。另一种方法是把加密后的数字信号通过 D/A

变换器变换为加密的模拟话音，使其能够在窄带信道中传输，这种置乱方法称为模数模置乱体制。它有数字加密的优点，又能在窄带信道中传输。新近发展起来的无须帧同步的模数模体制有其独特的优点，本书将对这种体制及有关传输技术作较详细的介绍。当前，有线信道传输保密话音有两个关键技术有待进一步解决，即自适应回波抵消和自适应信道均衡。因此，本书有专章加以论述，并介绍一些行之有效的实用技术。最后介绍的是我们多年来研制的模数模语音装置，以用其总结有关理论和技术的应用。

1.2 消息的加密和传输

众所周知，对消息加密的目的就是要使高密级的消息能够安全地在开放型信道中传送。图 1.2 是一般保密通信系统的物理模型。下面介绍该系统传递消息的过程。

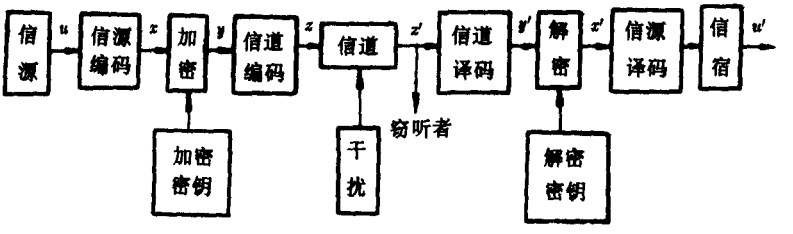

图 1.2 保密通信系统的物理模型

信源代表向保密通信系统提供消息 u 的人或机器。信源本身是十分复杂的，我们感兴趣的是它的输出消息 u'。输出消息 u' 可以有多种形式，总体可归纳为两类：(1)离散消息，例如由字母、文字、数据等组成的符号序列(或单个符号)；(2)连续消息，例如话音、图像和在时间上连续变化的消息参数等。由于通信系统的接收者(信宿)在收到消息之前并不知道信源将发出怎样的消息，所以一般地说信源发出的是随机性的消息，但因信源发出的消息都携

此为试读，需要完整PDF请访问：www.ertongbook.com

带着信息，消息的变化是有一定规律性的，因此严格地说信源发出的消息并不是完全随机性的。

信宿是消息传输的对象，它可以是接收消息的人或机器。根据实际需要，信宿接收的消息 u' 可以与信源发出的消息 u 相同，也可以不同。当两者形式不相同时，u' 是 u 的一个映射。

信道是传输消息的通道，又是传送物理信号的具体媒质。它可以是一对导线、一条同轴电缆或光导纤维或传输电磁波的空间等。就无线电通信而言，图 1.2 的信道是由发信机（调制器和发射机）、收信机（解调器和接收机）、天线和传输信号的媒质等四部分组成。这种信道的输入信号和输出信号都是基带信号。收、发信机又称为信道机。发信机把基带信号变换成为便于传输媒质的射频大功率信号，而收信机则是把射频信号恢复成为所需要的基带信号。一般信道都属于开放信道。不论是指定的接收者或是窃听者都可同样方便地收到在开放信道中传输的消息。所不同的是指定的接收者由于掌握解密的手段，因此能把接收到的加密消息正确地恢复为明文消息；而其他接收者则因未掌握解密手段而不能把所收到的加密消息进行解密。与开放信道相反的是秘密信道，它是用来传送密钥的通道，它可以是秘密专线甚至是由信使来传送更换密钥的信息。

信源编码器能把信源发出的消息变换成由二进制码元（或多进制码元）组成的代码组，这种代码组就是基带信号。此外，信源编码还能起着压缩信源的冗余度以提高通信效率的作用。例如，声码器就是实用的例子。信道编码器的作用是在信源编码器输出的代码组上有目的地增加一些监督码元，使之具有检错或纠错的能力。这实质上是增加一种可资利用的冗余度，来提高消息传输的可靠性。信道译码器能将落在编码序列的检错或纠错范围内的错传码元检出或纠错，从而提高了信道传输消息的可靠性。信源译码器能把信道译码器输出的代码组变换成信宿所需要形式的消息。它的译码过程相当于信源编码的逆操作。

干扰源是整个通信系统中各种干扰的集中反映，用以表示消息在信道中传输时遭干扰的情况。对于任何通信系统而言，干扰的性质、大小是影响系统通信可靠性的主要因素。

密钥源是产生密钥 k 的源。信道编码器的输出信号 x 经过密钥 k 的加密运算后，就把明文消息 x 变换为密文消息 y。若窃听者未掌握发端所采用的密钥 k，他就很难将所窃听到的信号 z' 解成明文。而收端的信宿则因知道预先约定的密钥 k，因此能方便地将收到的信号 z' 解成明文。对二进制数字代码而言，加密相当于 $y=z\oplus p$ 运算(其中序列 p 通常是由密钥 k 控制的伪随机序列)。而解密则相当于 $x'=y'\oplus p$ 运算。这里 x'，y'，z' 之所以不同于发端的 x，y，z 是考虑到信号在信道中传输时受到干扰的影响。但在正常条件下，总会有 $x'\approx x$，$y'\approx y$，$z'\approx z$ 的情况。

若密文窃听者通过艰巨分析能够从所窃听到的信号 z' 中解出明文，我们称这种过程为破译。破译的结果是窃密者掌握了发端所采用的密钥 k。

1.3 保密通信、信息论、密码学之间的关系

从图 1.2 可以清楚地看到：保密通信系统采取了信源编码、信源加密和信道编码等措施，使得在信道中传输的消息具有抗信道干扰和防止消息被非法接收者或无关人员窃听的能力，从而能够安全、可靠地把消息传送给指定的接收者。

香农信息论是在信息可以量度的基础上，研究有效地、可靠地传递消息的科学。它涉及到信息量度、信息特性、信息传输速率、信道容量、干扰对消息可靠传输的影响等方面的知识。而密码学则是研究如何隐蔽消息的信息内容以便加密消息在开放信道传输时不被窃听的科学。它涉及到加密体制、保密性量度、消息的统计特性及破译等方面的知识。由此可见，信息论和密码学是保密通信传输消息的两个不同侧面的理论基础。这就是香农在 40 年代同时研究

信息论和密码学的原因。香农在1948年发表的《通信的数学理论》奠定了信息论的基础。此后，又在1949年发表的《保密系统的通信理论》奠定了现代密码通信的基础。这是一篇用信息论观点来讨论密码通信问题的论文。他对密码通信的重要贡献之一，是提出了密码通信系统的模型，把各种各样的加密体制概括为分别处在收、发两端的一对加、解密变换器；而把整个系统概括为一条受密钥控制的加、解密变换和传输由这种变换所形成消息的开放信道，以及一条专门用来传输密钥的秘密信道。这样就可用数学模型法和信息论来对任意一个密码通信系统进行定量分析，使定量地评价不同密码体制的优劣成为可能。

香农对密码通信的另一重大贡献是他的理论中引入熵和保密度两个重要概念。前者是信息量度的标准，后者则是安全通信的重要指标。人们不仅可以根据这两个物理量对任何一个密码通信系统的安全性进行定量评估，而且也是设计新的保密通信系统的重要依据。

我们在上节已经提到过，信源编码的作用在于压缩消息中的冗余度以资降低消息的数码率，从而可把节省下来的比特数，用来增加有纠错能力的码元以提高消息在信道中传输的可靠性，又不致于降低信息的传输速率。这是因为信源编码压缩了消息中那些在收端译码器难以发挥抗信道干扰的冗余度，而信道编码则是在消息中增加一些收端译码容易实现抗信道干扰的冗余度。由于收端译码器是根据信道编码的逆操作进行译码的，因此能够发挥这种冗余度的潜在抗信道干扰的能力。

我们也可认为加密措施也是增加消息序列的冗余度。然而由加密增加的冗余度并没有提高消息序列抗信道干扰的潜力，而是对信道传输的消息起着掩盖作用，使非法接收（窃听）者或无关人员不能从所收到的加密消息中解出明文消息，而指定的接收者则因事先掌握发端使用的密钥，因而能够将收到的加密消息正确地解密。为了使这种冗余度有别于信息论的冗余度，此处把它称为模

糊度。它和密钥量或密钥空间的大小都可用来表明密码通信系统的保密度。

熵是信息论用来表征信源中任一符号消息所携带的平均信息量，也是唯一地确定信源中任一符号消息时所需要的最小平均信息量。信源消息的冗余度是指该消息可被压缩到不失去原意的程度。若该消息的实际熵为 $H_R(x)$，而信源熵为 $H(x)$，则该消息的冗余度可以用 $H_R(x)-H(x)$ 表示。由此可见，增加密钥量和减少冗余度是提高密码通信系统保密度的有效措施。

第 2 章　密码通信的数学基础

2.1 引　　言

上章已经提到香农的密码通信系统模型把各种密码体制的功能通过一对加、解变换器来实现。这种变换的具体性能可由某一种数学变换加以描述。采用现代计算机技术能方便地实现这种变换，这也是现代密码装置广泛采用快速微处理器的原因之一。由于现代密码通信系统的保密性，设备的复杂性，甚至设备的体积、重量、价格等都和所采用的密码体制及其加、解密技术密切相关，因此选择合适的数学变换及相应的计算技术是设计实用密码通信的核心问题。由此可见，打好密码学的数学基础是掌握密码理论及其实用技术的必由之路。限于篇幅，本章着重介绍一般工程技术人员不够熟悉的密码学的重要数学基础知识。它们是：密码学的代数基础；快速数论变换、快速离散富里叶变换以及大阶数矩阵的一些运算技巧。

2.2 数论的基本知识

数论是研究数的规律，特别是整数的运算规律。本节将简要介绍整数的分解、同余式的基本性质及解同余式的方法。

2.2.1 整数的分解

1) 整数的整除性及有关定义

(1) 设 a，b 是任意两个整数，$b\neq 0$，并且有另一整数 q，使得 a

$=bq$ 成立。则 b 能整除 a，记作 $b|a$，这样 a 是 b 的倍数，而 b 则是 a 的因数(或约数)。若该等式不成立，则 b 不能整除 a，记作 $b\nmid a$。

(2) 设 a,b 是任意两个整数且 $b>0$，若有两个唯一整数 q 和 r，使得 $a=bq+r$ 成立，其中 $0\leqslant r<b$，则称 r 为整数模 b 的最小非负剩余，记作 $((a))_b=r$ 或 $a\equiv r \bmod b$。称 q 为不完全商数或"商数"。显然，当 $r=0$ 时，则 $b\nmid a$，而当 $r\neq 0$ 时，则 $b\nmid a$。

(3) 若 $a_1,a_2,\cdots,a_n$ 是 n 个整数，用 $n>2$，d 是它们中每个数的约数，则称 d 为 $a_1,a_2,\cdots,a_n$ 的一个公约数，所有公约数中最大的那一个称为最大公约数(或最大公因数)，记作 $\gcd(a_1,a_2,\cdots,a_n)$ 或简写为 $(a_1,a_2,\cdots,a_n)$。若 $(a_1,a_2,\cdots,a_n)=1$，则意味着 $a_1,a_2,\cdots,a_n$ 是互素，因为它们之间除了 1 没有其他公因子。若任意两个 a_i 和 $a_j(1\leqslant i,j\leqslant n)$ 有 $(a_i,a_j)=1$，则称 $a_1,a_2,\cdots,a_n$ 两两互素。若 m 是 $a_1,a_2,\cdots,a_n$ 诸数的倍数，则称 m 是这 n 个数的公倍数。所有公倍数中最小的正数，称为最小公倍数，记作 $\mathrm{Lcm}(a_1,a_2,\cdots,a_n)$ 或 $[a_1,a_2,\cdots,a_n]$。显然，当正整数 $a_1,a_2,\cdots,a_n$ 两两互素时，则有 $[a_1,a_2,\cdots,a_n]=a_1a_2a_3\cdots a_n$。

(4) 余数的一些重要性质

① 若 n,i,d 是任意整数，用 $d\nmid n$，则经模 d 运算后的余数 $R_d(n)=r$ 有如下基本性质：

$$R_d(n+id)=R_d(n)=r \tag{2.1}$$

这是因为 $R_d(n+id)=R_d[(q+i)d+r]=r$。

例 1 $R_5=(-13+3\times 5)=R_5(2)=2$

$R_3(100)=R_3(1+33\times 3)=R_3(1)=1$

值得指出的是

$$R_d(n)=R_{-d}(n) \tag{2.2}$$

因为 $n=qd+r$，所以运算时只是 d 的符号有变化，而余数不变。

例 2 $R_7(50)=R_7(2\times 7+1)=R_{-7}(1)=1$，但若 $r<1$，则有

$$R_d(n)=R_d(r)=R_d(d+r)$$

例 3 当 $n=-13=-2\times 5-3=-3\times 5+2$ 时，则

此为试读，需要完整PDF请访问：www.ertongbook.com