全国高技术重点图书·通信技术领域

纠错密码理论

王新梅　马文平　武传坤　著

人民邮电出版社

图书在版编目(CIP)数据

纠错密码理论/王新梅,马文平,武传坤著 . -北京:人民邮电出版社,2001.3

全国高技术重点图书·通信技术领域

ISBN 7-115-08896-9

Ⅰ.纠… Ⅱ.①王…②马…③武… Ⅲ.纠错码-通信理论 Ⅳ.TN911.22

中国版本图书馆 CIP 数据核字(2000)第 76617 号

全国高技术重点图书·通信技术领域

纠错密码理论

◆ 著 王新梅 马文平 武传坤

责任编辑 徐修存 王亚明

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号

邮编 100061 电子函件 315@pptph.com.cn

网址 http://www.pptph.com.cn

读者热线 010-67129212 010-67129211(传真)

北京汉魂图文设计有限公司制作

北京朝阳隆昌印刷厂印刷

新华书店总店北京发行所经销

◆ 开本:850×1168 1/32

印张:9.25

字数:236 千字 2001 年 3 月第 1 版

印数:1-4 000 册 2001 年 3 月北京第 1 次印刷

ISBN 7-115-08896-9/TN·1654

定价:25.00 元

内 容 提 要

本书是关于密码和纠错码基本理论的一本专著。书中介绍了纠错码中的 NPC 问题，论述了基于纠错码的公钥密码体制、身份认证方案和私钥密码体制，详细地讨论了这些方案的安全性，讨论了纠错码数字签名技术，论述了有关签名方案的安全性，对纠错码和认证码的关系进行了详细的论述，给出了由纠错码构造认证码和由认证码构造纠错码的方法，论述了密钥分散管理和纠错码的关系，介绍了置换密码理论。

本书可供从事通信理论、信息论、编码学、密码学和数学科研与教学的有关人员学习参考。

《全国高技术重点图书》
出版指导委员会

《全国高技术重点图书·通信技术领域》
编审委员会

序(一)

1948 年 C.E.Shannon 在《通信的数学理论》一文中提出了著名的信道编码定理,开创了纠错码的研究方向,此文标志着编码理论的开端。1949 年,C.E.Shannon 在他的论文《保密系统的通信理论》中,从信息论的角度阐述了密码学的基本问题,从而奠定了现代密码学的研究基础。自此以来,几十年间,纠错码和密码学一直在不同的领域中互不相干地向前发展。70 年代中期,Diffie 和 Hellman 在他们的论文《密码学的新方向》中,提出加密和解密密钥不同的公钥密码体制的思想,并基于离散对数问题,提出了第一个公钥密码系统,随后,很多学者构造了许多不同的基于数学难解问题的公钥密码系统,如 RSA、背包体制、ElGamal 方案等。1978 年 Berlekamp 等证明了一般线性分组码的译码问题是一个 NPC 问题,从而为纠错码在密码中的应用打开了大门,同年,MacEliece 利用 Goppa 码构造了第一个基于线性分组码的公钥密码体制。从此以后,国内外很多学者利用纠错码的特点和理论构造了各种各样的公钥密码体制、数字签名方案、秘密共享方案、认证码等,纠错码和密钥相结合的研究得到了迅速的发展。

王新梅教授和他的学生们组成的科研组,是我国最早从事纠错码、纠错码和密码相结合的研究组织之一。早在 80 年代中期,他们就开始从事纠错码和密码相结合的研究工作。在近 20 年的研究中,在国家自然科学基金、博士点基金和密码发展基金的资助下,他们取得了一系列成果,如 Xinmei 数字签名方案是第一个基于纠错码的数字签名方案,这些都是具有国际水平的工作。本书是这方面研究工作的总结,其中很多内容是他们的研究成果,也是我国第一本比较全面和系统地阐述纠错码在密码学中的应用的书籍,全书叙述比较系

统、全面、内容新颖。我相信本书的出版，将促进我国密码学和纠错码的发展以及它们相结合的研究。

王新梅教授等所著《纠错密码理论》一书的出版，使我不禁想起十年前我的老友吴伯修教授等所著的《信息论与编码》，该书在把信息论基础、纠错码理论和保密通信三部分综合在一起方面，开创了先河。（该书于 1990 年完成，东南大学出版社出版，由我负责主审）。十年过去了，王新梅教授的《纠错密码理论》一书反映了我国在这一领域有了很大进展。自古长江后浪推前浪。我们年轻一代，一定会在今后把这一领域的工作推向新的高度。

陈太一

序(二)

纠错码和密码学可以说是信息科学领域中的一对孪生兄弟。纠错码的任务是通过增加消息多余度的办法排除在噪声信道下传输消息时所带来的干扰,从而使接收端能够纠正错误,正确译码。与此相反,密码学的任务则是人为地在要传输的消息中加入"噪声",使其变形成窃听者难于解读的消息,而收端则可通过"密钥"将消息正确解密。

自从 C.E.Shannon 在 1948 及 1949 年分别发表了两篇著名论文 *A mathematical theory of communication* 及 *Communication theory of secrecy* 以来,纠错码与密码学始终各自独立地并行发展。70 年代末,R.J.McEliece 首先将纠错与加密结合起来,提出了一种基于纠错码的公钥体制。近 20 年来,国内外一些学者沿着这条道路开展了纠错码与密码相结合以寻求构造新的密码体制及认证方案的研究。王新梅教授及其学生们在这一研究方向上做了许多有价值的工作。本书在这一基础上系统地总结了纠错码与密码相结合的研究成果,其中包括了王新梅教授及其学生们在这一领域的工作。我相信,这本专著的出版对我国学者开展密码学领域的研究工作会起到一定的推动作用。

肖国镇

前　言

纠错码和密码学是两门不同的学科，在70年代以前，它们几乎互不相关，各自独立地向前发展。1976年W.Diffe和M.E.Hellman发表了在密码学领域中具有里程碑意义的文章——《密码学的新方向》，提出了新的密码思想，使得密码体制的安全性常常建立在某个难解的数学问题之上，即NPC问题之上。1978年E.R.Berlekamp，R.J.McEliece和H.C.A van Tilborg证明了纠错码中一般线性分组码的译码问题是一个NPC问题。这两项成果建立起纠错码和密码学相结合的理论基础。1978年R.J.McEliece根据一般线性分组码的译码问题是一个NPC问题，Goppa码具有快速译码算法的特点，首次构造了基于纠错码的公钥密码体制，简称为McEliece体制。从此以后，有关纠错码和密码相结合的研究，特别是利用纠错码构造各种密码体制和认证方案得到了迅速的发展。

本书主要论述纠错码和密码相结合方面的研究结果。前两章介绍阅读本书需要的密码知识，讲述了密码系统和认证系统中的基本概念和有关的信息论基础，介绍了著名的密码方案；第三章介绍有关纠错码的基础知识、复杂性理论以及纠错码中的NPC问题；第四章讨论基于纠错码的公钥密码体制和基于纠错码的认证方案，详细讨论了这些方案的安全性；第五章讨论了基于纠错码的私钥密码体制及其安全性；第六章讨论了纠错码数字签名方案，论述了Xinmei方案，并讨论了其安全性，对其进行了改进；第七章论述了密钥分散管理和纠错码的关系，并给出由级连码等构造密钥共享方案的方法；第八章介绍了置换密码理论；第九章详细论述了消息认证码和纠错码的关系，研究了认证码的组合结构，给出了由纠错码构造认证码和由

认证码构造纠错码的方法;第十章介绍了 Cartesian 认证码和纠错码。

本书大部分内容是我们完成的两个国家自然科学基金资助项目——"纠错与加密相结合的研究"和"认证码的研究"的科研成果的总结。为了保持全书的系统性,我们也介绍了有关的国内外研究成果。

我们感谢参与两个自然科学基金资助项目研究的所有研究人员,特别是美国 IBM 公司的李元兴博士和荷兰爱因豪芬大学的徐胜波博士;感谢近几年来编码和密码讨论班中的所有老师和研究生,特别是肖国镇教授和王育民教授。多年来,在这个集体中我们不仅共同学习,讨论新思想、新理论和新技术,而且在精神上也得到了很大的鼓舞和支持。同时,我们要感谢我们的导师陈太一院士,他始终如一地支持、鼓励我们在这方面进行不断的探索。最后我们还要感谢人民邮电出版社的徐修存和王亚明两位编辑,没有他们的大力支持和精心编辑,本书是不可能出版的。感谢吉士琴工程师细心、认真地打印全稿。谨以此书献给所有关心过我们的同志们。

本书第一、三、六章由王新梅执笔,第七、八、九章由武传坤执笔,第二、四、五、十章由马文平执笔,王新梅统编全稿。

由于作者水平有限,错误遗漏在所难免,恳请读者批评指正。

本书得到国家自然科学基金的资助。

编　者

目　录

第一章　通信保密系统

保密学或者从比较窄范围内讲的密码学，是一门研究通信安全和保护信息资源的既古老而又年青的科学和技术。它包括两方面：密码编码学和密码分析学。密码编码学是对信息编码以隐蔽信息的一门学问；而密码分析学是研究分析破译密码的学问。这二者既相互对立又相互促进，共同推动密码学的发展。

纠错码是提高通信质量或可靠性的一门年青的学科。自 1948 年 Shannon 提出信道编码定理至今[1]，这门学科已取得了丰硕的成果。利用纠错码的差错控制技术，已成为通信系统设计中的一种重要、在某些场合甚至是必不可少的技术手段，纠错编译码器已成为现代通信系统中的重要组成部分。

纠错码与密码学是两门不同的学科。在 70 年代以前它们几乎互不相关各自独立的向前发展。1976 年 Diffie 和 Hellman 发表了在密码学领域内具有里程碑意义的文章[2]，他们提出了公开密钥密码体制（简称公钥体制）。1978 年 Berlekamp、McEliece 和 Tilborg 等证明了纠错码理论中一般线性码的译码等问题是 NPC 问题[3]，同年 McEliece 利用纠错码构造了第一个公钥密码体制[4]。自此以后，有关密码学与纠错码相结合的研究，利用纠错码构造各种密码系统和认证系统的研究得到了迅速发展，从而把这两门原本无关的学科结合在一起。

这一章我们首先介绍密码编译码器和纠错码编译码器在整个通信系统或信息传输系统中的地位，然后介绍密码系统中的某些最基本的概念和术语以及衡量密码系统安全性的某些有关问题，以便为以后的讨论奠定必要的基础。

1.1 通信系统模型

所有信息传输、存储系统如通信、雷达、遥测遥控、计算机的内外存储系统和内部运算，以及计算机通信网中的信息传输等，都可归结成如图 1.1 所示的数字通信系统模型。

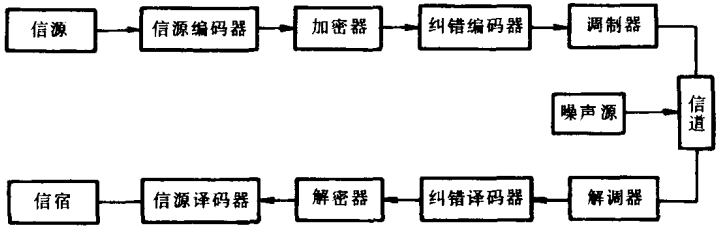

图 1.1 数字通信系统模型

信息传输或通信的目的，是要把收方不知道的信息及时、可靠、完整、安全而又经济地传送给指定的收方。图 1.1 中所描述的整个系统的各部分，就是为了完成上述目的。当然，由于具体要求及应用场合的不同，图中的某些组成部分可能没有，也可能还要增加其它部分。图中信源编码器是把信源（人、计算机或其它信息处理设备）发出的消息如语音、图像、文字等转换成二进制形式的信息序列，也就是 0、1 符号串，并且为了使传输更为经济有效，还要去掉一些与被传信息无关的多余度。

在信息传输或处理过程中，除了指定的接收者外，还有非指定的或非授权的用户，他们通过各种技术手段企图窃取机密信息。因此，为了保证被传送信息的安全和隐私，必须在信源编码器输出通过加密器时，用编码方法对信息进行隐藏。由于传输信息的媒质如电波、有线等总是存在有各种人为或天然的干扰和噪声，因此，为了提高整个通信系统传输信息的可靠性，就需要对加密器输出的信息进行一次纠错编码，人为地增加一些多余信息，使其具有自动检错或纠错功能。这种功能由图中的纠错编码器完成。为了使信息能与传输媒质