国外电子与通信教材系列

CDMA蜂窝移动通信与网络安全

CDMA Cellular Mobile Communications and Network Security

[韩] Man Young Rhee 著
袁超伟 等译

PH PTR
電子工業出版社
Publishing House of Electronics Industry
www.phei.com.cn

国外电子与通信教材系列

CDMA蜂窝移动通信与网络安全

CDMA Cellular Mobile Communications and Network Security

[韩] Man Young Rhee 著

袁超伟 等译

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内容简介

本书主要介绍了CDMA原理与系统，能够满足各种层次人员的需要。CDMA的网络安全是本书的特色。本书采用了大量的实例和数学运算来帮助读者理解CDMA蜂窝系统、消息加密和网络安全。全面而系统地讲述了CDMA信道操作技术，反向和前向CDMA信道，移动台呼叫处理，基站呼叫处理，单向Hash函数和消息摘要，鉴权、加密和识别，前向和反向W-CDMA信道。

本书适用于从事CDMA蜂窝系统深入研究与开发的电信工程师、工程管理人员，同时对在这个领域进行教学、研究、开发的教师、学生有很好的参考价值。

版权贸易合同登记号：图字：01-2001-5087

图书在版编目（CIP）数据

CDMA蜂窝移动通信与网络安全/（韩）曼扬里著；袁超伟等译. -北京：电子工业出版社，2002.5
（国外电子与通信教材系列）
书名原文：CDMA Cellular Mobile Communications and Network Security
ISBN 7-5053-7614-4

Ⅰ.C... Ⅱ.①曼... ②袁... Ⅲ.码分多址-移动通信-通信网-安全技术 Ⅳ.TN929.533

中国版本图书馆CIP数据核字（2002）第031872号

责任编辑：李秦华　陶淑毅
印 刷 者：中国科学院印刷厂
出版发行：电子工业出版社　http://www.phei.com.cn
　　北京市海淀区万寿路173信箱　邮编：100036
经　　销：各地新华书店
开　　本：787×1092　1/16　　印张：24.75　字数：634千字
版　　次：2002年5月第1版　　2002年5月第1次印刷
定　　价：37.00元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077

序

2001 年 7 月间，电子工业出版社的领导同志邀请各高校十几位通信领域方面的老师，商量引进国外教材问题。与会同志对出版社提出的计划十分赞同，大家认为，这对我国通信事业、特别是对高等院校通信学科的教学工作会很有好处。

教材建设是高校教学建设的主要内容之一。编写、出版一本好的教材，意味着开设了一门好的课程，甚至可能预示着一个崭新学科的诞生。20 世纪 40 年代 MIT 林肯实验室出版的一套 28 本雷达丛书，对近代电子学科、特别是对雷达技术的推动作用，就是一个很好的例子。

我国领导部门对教材建设一直非常重视。20 世纪 80 年代，在原教委教材编审委员会的领导下，汇集了高等院校几百位富有教学经验的专家，编写、出版了一大批教材；很多院校还根据学校的特点和需要，陆续编写了大量的讲义和参考书。这些教材对高校的教学工作发挥了极好的作用。近年来，随着教学改革不断深入和科学技术的飞速进步，有的教材内容已比较陈旧、落后，难以适应教学的要求，特别是在电子学和通信技术发展神速、可以讲是日新月异的今天，如何适应这种情况，更是一个必须认真考虑的问题。解决这个问题，除了依靠高校的老师和专家撰写新的符合要求的教科书外，引进和出版一些国外优秀电子与通信教材，尤其是有选择地引进一批英文原版教材，是会有好处的。

一年多来，电子工业出版社为此做了很多工作。他们成立了一个“国外电子与通信教材系列”项目组，选派了富有经验的业务骨干负责有关工作，收集了 230 余种通信教材和参考书的详细资料，调来了 100 余种原版教材样书，依靠由 20 余位专家组成的出版委员会，从中精选了 40 多种，内容丰富，覆盖了电路理论与应用、信号与系统、数字信号处理、微电子、通信系统、电磁场与微波等方面，既可作为通信专业本科生和研究生的教学用书，也可作为有关专业人员的参考材料。此外，这批教材，有的翻译为中文，还有部分教材直接影印出版，以供教师用英语直接授课。希望这些教材的引进和出版对高校通信教学和教材改革能起一定作用。

在这里，我还要感谢参加工作的各位教授、专家、老师与参加翻译、编辑和出版的同志们。各位专家认真负责、严谨细致、不辞辛劳、不怕琐碎和精益求精的态度，充分体现了中国教育工作者和出版工作者的良好美德。

随着我国经济建设的发展和科学技术的不断进步，对高校教学工作会不断提出新的要求和希望。我想，无论如何，要做好引进国外教材的工作，一定要联系我国的实际。教材和学术专著不同，既要注意科学性、学术性，也要重视可读性，要深入浅出，便于读者自学；引进的教材要适应高校教学改革的需要，针对目前一些教材内容较为陈旧的问题，有目的地引进一些先进的和正在发展中的交叉学科的参考书；要与国内出版的教材相配套，安排好出版英文原版教材和翻译教材的比例。我们努力使这套教材能尽量满足上述要求，希望它们能放在学生们的课桌上，发挥一定的作用。

最后，预祝“国外电子与通信教材系列”项目取得成功，为我国电子与通信教学和通信产业的发展培土施肥。也恳切希望读者能对这些书籍的不足之处、特别是翻译中存在的问题，提出意见和建议，以便再版时更正。

吴佑寿

中国工程院院士、清华大学教授

“国外电子与通信教材系列”出版委员会主任

出 版 说 明

进入21世纪以来，我国信息产业在生产和科研方面都大大加快了发展速度，并已成为国民经济发展的支柱产业之一。但是，与世界上其他信息产业发达的国家相比，我国在技术开发、教育培训等方面都还存在着较大的差距。特别是在加入WTO后的今天，我国信息产业面临着国外竞争对手的严峻挑战。

作为我国信息产业的专业科技出版社，我们始终关注着全球电子信息技术的发展方向，始终把引进国外优秀电子与通信信息技术教材和专业书籍放在我们工作的重要位置上。在2000年至2001年间，我社先后从世界著名出版公司引进出版了40余种教材，形成了一套“国外计算机科学教材系列”，在全国高校以及科研部门中受到了欢迎和好评，得到了计算机领域的广大教师与科研工作者的充分肯定。

引进和出版一些国外优秀电子与通信教材，尤其是有选择地引进一批英文原版教材，将有助于我国信息产业培养具有国际竞争能力的技术人才，也将有助于我国国内在电子与通信教学工作中掌握和跟踪国际发展水平。根据国内信息产业的现状、教育部《关于“十五”期间普通高等教育教材建设与改革的意见》的指示精神以及高等院校老师们反映的各种意见，我们决定引进“国外电子与通信教材系列”，并随后开展了大量准备工作。此次引进的国外电子与通信教材均来自国际著名出版商，其中影印教材约占一半。教材内容涉及的学科方向包括电路理论与应用、信号与系统、数字信号处理、微电子、通信系统、电磁场与微波等，其中既有本科专业课程教材，也有研究生课程教材，以适应不同院系、不同专业、不同层次的师生对教材的需求，广大师生可自由选择和自由组合使用。我们还将与国外出版商一起，陆续推出一些教材的教学支持资料，为授课教师提供帮助。

此外，“国外电子与通信教材系列”的引进和出版工作得到了教育部高等教育司的大力支持和帮助，其中的部分引进教材已通过“教育部高等学校电子信息科学与工程类专业教学指导委员会”的审核，并得到教育部高等教育司的批准，纳入了“教育部高等教育司推荐——国外优秀信息科学与技术系列教学用书”。

为做好该系列教材的翻译工作，我们聘请了清华大学、北京大学、北京邮电大学、东南大学、西安交通大学、天津大学、西安电子科技大学、电子科技大学等著名高校的教授和骨干教师参与教材的翻译和审校工作。许多教授在国内电子与通信专业领域享有较高的声望，具有丰富的教学经验，他们的渊博学识从根本上保证了教材的翻译质量和专业学术方面的严格与准确。我们在此对他们的辛勤工作与贡献表示衷心的感谢。此外，对于编辑的选择，我们达到了专业对口；对于从英文原书中发现的错误，我们通过与作者联络、从网上下载勘误表等方式，逐一进行了修订；同时，我们对审校、排版、印制质量进行了严格把关。

今后，我们将进一步加强同各高校教师的密切关系，努力引进更多的国外优秀教材和教学参考书，为我国电子与通信教材达到世界先进水平而努力。由于我们对国内外电子与通信教育的发展仍存在一些认识上的不足，在选题、翻译、出版等方面的工作中还有许多需要改进的地方，恳请广大师生和读者提出批评及建议。

电子工业出版社

教材出版委员会

关于《CDMA蜂窝移动通信与网络安全》一书

《CDMA蜂窝移动通信与网络安全》一书（CDMA Cellular Mobile Communications and Network Security）是一本CDMA（码分多址）蜂窝移动通信方面实用性很强的参考书。

CDMA技术是当前无线电通信，尤其是移动通信的主流技术，不论是在中国已经建设的IS-95规范的中国联通CDMA网、各大移动通信运营商正准备试验及建设的第三代（3G）系统还是大设备研发商已经在开发的三代以后（Beyond 3G，也称4G）更宽带宽的移动通信系统，CDMA技术都是主要选择。

本书对IS-95规范的窄带CDMA通信系统做了较详细的介绍，从系统构成、扩频通信系统的调制、多址、卷积编码、交织、沃氏（Walsh）函数扩展、直接序列扩展、长码产生、扰码、鉴权和保密、信息加密和安全、反向信道、前向信道等等，均有具体的、数字举例的描述。后几章则详细讲述了移动台和基站的呼叫过程（包括各种状态：移动台初始化状态、空闲状态、系统接入状态、对业务信道的控制状态）、基站的导频和同步信道处理、寻呼信道处理、接入信道处理、业务信道处理、切换过程、移动台鉴权、识别等等。最后两章介绍了宽带CDMA（W-CDMA）的反向及前向信道。

可见，本书对CDMA的具体技术，尤其是IS-95标准的技术实现有具体说明。对CDMA网络运营人员、规划设计人员、研究开发人员、大学教师及研究生等均是一本极好的实用参考书，值得一看，还可供工作中查阅。

总参通信部副部长
中国电子学会会士、副理事长
中国通信学会常务理事
“国外电子与通信教材系列”出版委员会副主任

杨千里

译 者 序

20世纪90年代以来，移动通信发展迅速，我国现已有移动用户1.5亿。码分多址(CDMA)技术以它在系统容量、业务质量、安全性和可靠性等方面的优势倍受关注，全球已有近50个国家采用CDMA技术提供电信业务。新建成的中国联通CDMA网一期工程总投资240亿元人民币，采用IS-95A增强型技术标准，网络规模为1515万户覆盖全国31个省市的330个本地网，除开通基本通话业务和各种附加功能外，还开通移动智能网和短消息网等增值业务。七城市的IX试验网规模总容量为10万户，已经和正在开展高速上网、图像下载、可视电话等新业务试验。CDMA是一种先进的数字通信技术，经历了从窄带CDMA(IS-95 CDMA)向宽带CDMA的演进，已成为第三代移动通信系统的实际应用技术。

本书全面而系统地介绍了CDMA原理与系统，能够满足各种层次人员的需要，CDMA的网络安全是本书的特色。本书采用了大量的实例和数学运算来帮助读者理解CDMA蜂窝系统、消息加密和网络安全。

本书适用于从事CDMA蜂窝系统方面深入研究与开发的电信工程师、工程管理人员，同时对在这个领域进行教学、研究、开发、应用的教师和学生有很好的参考价值。

参与本书翻译工作的有袁超伟、张元雯、陈文杰、王桃荣、刘静、徐冬云、孙楠、章高男、张元馨等。同时，该书的翻译工作还得到了所在部门和相关领导的大力支持，在此一并表示感谢。受译者水平所限，错误和不妥之处在所难免，恳请读者批评指正。

前　言

本书主要讨论了 CDMA(码分多址)技术。作为未来移动通信系统前景广阔的技术,CDMA 正得到广泛的关注。

对于蜂窝系统而言,选择最恰当的接入方式是很具挑战性的工作。对于宽带服务,CDMA 是一种很有吸引力的无线接入技术。为了迎接这种挑战,必须熟悉 CDMA 数字蜂窝系统的相关技术和系统体系结构。

在过去的 6 年中,无线通信领域业已发生了巨变。本书旨在激发读者进一步探索这个极具挑战性的领域。1990 年初,由位于美国加利福尼亚圣迭戈的 QUALCOMM 股份有限公司(高通公司)先驱性地引入了关于 CDMA 扩频数字蜂窝系统概念和开创性的实现方法。该 CDMA 系统后来得到相关标准化组织的认可,已成为电信工业协会(TIA)和电子工业协会(EIA)的 IS-95 标准。

本书给出了全面的分析方法,有助于从业工程师规划和设计高效的 CDMA 蜂窝组网。本书也适合研究生学习扩频蜂窝系统的基本原理。本书中给出的大部分内容,特别是 CDMA 信道结构,均包含在 IS-95 原理和系统体系结构中。

本书中大量计算例子以数值表示,为的是让初学者更好地理解 CDMA 蜂窝系统。

下面是本书每章内容的摘要。

第 1 章概述了 CDMA 蜂窝系统的介绍性材料,简单解释了基于扩频系统的调制和多重接入技术。

第 2 章介绍了 CDMA 信道操作所需的最基本和实用的技术基础。

第 3 章和第 4 章涵盖了 CDMA 信道全面而详细的体系结构以及它们特性和功能的讨论。前向 CDMA 信道由导频、同步、寻呼和业务信道组成。导频信号是每个 CDMA 基站一直发送的不调制、直接序列扩频信号。移动台监视导频信道,以捕获前向 CDMA 信道定时并提供相关解调的相位参考。同步信道向移动台传送同步消息,为的是获得初始时间同步。寻呼信道也是经过编码、交织、扩频和调制的扩频信号,用来发送从基站到移动台的控制信息和寻呼信息。前向业务信道用来在通话过程中从基站向特定移动台发送用户数据和信令业务。除了导频信道,其他码道都经过了卷积编码、块交织、适当的 Walsh 函数正交扩频,再由导频 PN 序列正交对以 1.228 8 Mc/s 的速率扩展。

寻呼信道和前向业务信道也采用数据扰码技术。数据扰码在块交织器输出端以19.2 kb/s 进行。数据扰码通过对交织器输出字符与用户号码对应的长伪码进行模 2 加。长码是周期为 $2^{42}-1$ 的 PN 序列,用于前向 CDMA 信道(即寻呼和前向业务信道)的扰码和反向 CDMA 信道(即接入和反向业务信道)的扩频。反向 CDMA 信道由接入信道和反向业务信道组成。在反向 CDMA 信道上发送的所有数据都经过卷积编码、块交织、64 阶 Walsh 函数正交调制和长码片直接序列扩展再发送。反向业务信道使用数据脉冲随机发生器产生掩码数据 0 和 1,用来掩蔽码重复产生的冗余数据。

第 5 章和第 6 章描述的是基于高通系统包括切换过程的 CDMA 码道呼叫过程。

第 7 章给出了单向 Hash 函数和消息摘要的简明概要。无论对传统的对称算法还是公钥加密算法，单向函数是大多数协议的基本创建单元。单向 Hash 函数非常容易计算，但是极难逆运算。用于鉴权数据的 Hash 码算法是系统地排列的。

第 8 章讲述鉴权和消息保密。分析范围涉及大量由 152 比特 CDMA 蜂窝系统消息块到 18 比特 Hash 码的运算技术。移动台和基站协同操作对移动台进行鉴权。鉴权是这样一个过程，即信息在移动台和基站之间交互用于确认移动台身份。只有当能够表明移动台和基站处理的 SSD(共享加密数据)集相同的时候，鉴权过程才成功。SSD 是半永久存储在移动台存储器中的 128 比特长的共享加密数据。SSD 分为两个不同子集：SSD-A 和 SSD-B。前者用于支持鉴权过程；后者用于支持话音保密和消息加密。SSD 更新过程可以完全用 SSD-A-NEW 和 SSD-B-NEW 解释，并作为 SSD 产生输出。同时还包括信令消息加密和网络安全。

第 9 章和第 10 章介绍基于 JTC(AIR)/95 的宽带 CDMA 链路。反向和前向信息信道数据率为64 kb/s，32 kb/s 或 16 kb/s，PN 码片速率为 4.096 Mc/s，符号速率为 64 ks/s。

第 9 章讲述反向 W-CDMA 信道，它是从移动台到基站的通信链路。反向 W-CDMA 信道由接入信道和反向业务信道组成。接入信道包括反向导频信道和反向接入信道。反向业务信道包括三种不同信道：反向导频、信息和信令信道。反向业务信道上的所有数据都经过卷积编码、交织和直接序列扩展调制再发送。在第 10 章中，前向 W-CDMA 信道包括 1 路导频信道、1 路同步信道、最多 8 路寻呼信道和一定数量前向业务信道(如前向信息和信令信道)。这些码道中每一路都由适当的 Walsh 码正交扩展，然后以 4.096 Mc/s 固定码片速率的 PN 序列扩展。前向业务信道中的前向信令信道经过卷积编码、块交织、长码直接序列扩展、Walsh 函数正交扩展、以 4.096 Mc/s 固定码片速率的 PN 序列正交调制、基带滤波和 QPSK 波形发送。

本书可以作为帮助读者进行数字蜂窝系统技术方面深入研究和开发的基本教材。希望书中总结的带有完整解答的 148 个问题更有益于读者自学。在这个飞速发展的领域早期阶段写这本书确实是种很大的挑战。希望读者能发现书中存在的问题，真诚欢迎读者的反馈，这将有助于提高本书的再版质量。

目　录