信息安全技术与教材系列丛书

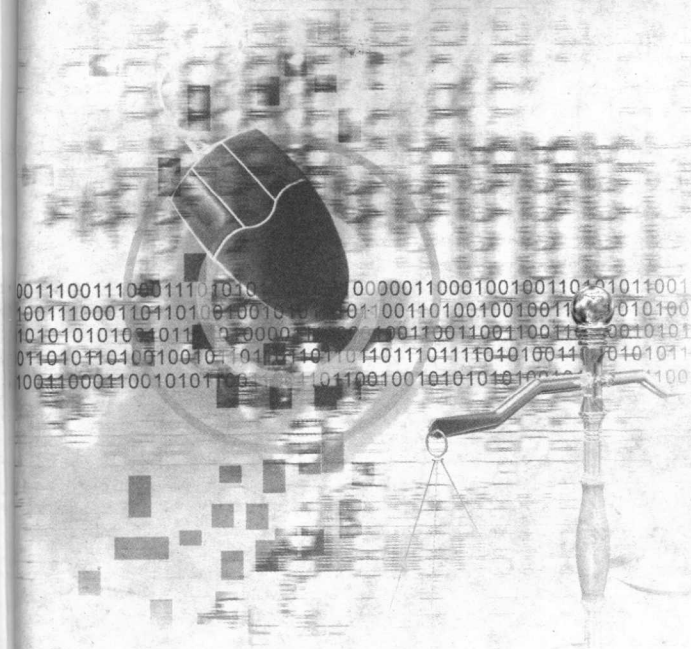
信息安全综合实验教程

张焕国　王丽娜 / 编著

WUHAN UNIVERSITY PRESS
武汉大学出版社

信息安全技术与教材系列丛书

国家自然科学基金重大研究计划项目（编号：90104005，90204011）
国家自然科学基金项目（编号：60473023，60373087）



信息安全综合实验教程

张焕国　王丽娜 / 编著

WUHAN UNIVERSITY PRESS
武汉大学出版社

图书在版编目(CIP)数据

信息安全综合实验教程/张焕国,王丽娜编著.—武汉:武汉大学出版社,2006.1

信息安全技术与教材系列丛书

ISBN 7-307-04689-x

Ⅰ.信… Ⅱ.①张… ②王… Ⅲ.信息系统—安全技术—高等学校—教材 Ⅳ.TP309

中国版本图书馆 CIP 数据核字(2005)第 119705 号

责任编辑:黄金文 杨 华 责任校对:刘 欣 版式设计:支 笛

出版发行:**武汉大学出版社** (430072 武昌 珞珈山)

(电子邮件:wdp4@whu.edu.cn 网址:www.wdp.whu.edu.cn)

印刷:湖北省孝感日报社印刷厂

开本:787×980 1/16 印张:26.75 字数:551 千字

版次:2006 年 1 月第 1 版 2006 年 1 月第 1 次印刷

ISBN 7-307-04689-x/TP·181 定价:38.00 元

信息安全技术与教材系列丛书

编　委　会

内容简介

信息安全技术是一种非常重要的信息技术。本书主要内容包括 FPGA 实验、DSP 实验、指纹识别、计算机电磁干扰测试、智能卡实验、Cisco 网管软件、计算机病毒分析与对抗、VPN 密码机、隔离网闸、IDS、Firewall、数字水印与软件水印、网络攻防实验。

本书可作为高等院校具有一定计算机基础的信息安全专业、密码学专业、计算机专业的研究生或高年级本科生实验教材，也可作为科研院所相关专业的科技工作者安全设计实验的参考书。

序 言

21 世纪是信息的时代，信息成为一种重要的战略资源。信息科学成为最活跃的学科领域之一，信息技术改变着人们的生活和工作方式，信息产业成为新的经济增长点。信息的安全保障能力成为一个国家综合国力的重要组成部分。

当前，以 Internet 为代表的计算机网络的迅速发展和“电子政务”、“电子商务”等信息系统的广泛应用，正引起社会和经济的深刻变革，为网络安全和信息安全开拓了新的服务空间。

世界主要工业化国家中每年因利用计算机犯罪所造成的经济损失远远超过普通经济犯罪。内外不法分子互相勾结侵害计算机系统，已成为危害计算机信息安全的普遍性、多发性事件。计算机病毒已对计算机系统的安全构成极大的威胁。社会的信息化导致新的军事革命，信息战、网络战成为新的作战形式。

总之，随着计算机在军事、政治、金融、商业等部门的广泛应用，社会对计算机的依赖越来越大，如果计算机系统的安全受到破坏将导致社会的混乱并造成巨大损失。因此，确保计算机系统的安全已成为世人关注的社会问题和计算机科学的热点研究课题。

信息安全事关国家安全，事关经济发展，必须采取措施确保信息安全。

发展信息安全技术与产业，人才是关键。培养信息安全领域的专业人才，成为当务之急。2001 年经教育部批准，武汉大学创建了全国第一个信息安全本科专业。到 2003 年，全国设立信息安全本科专业的高等院校增加到 20 多所。2003 年经国务院学位办批准武汉大学建立信息安全博士点。

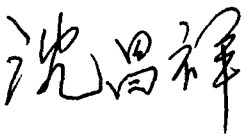
为了增进信息安全领域的学术交流、为信息安全专业的大学生提供一套适用的教材，武汉大学组织编写了这套《信息安全技术与教材系列丛书》。这套丛书涵盖了信息安全的主要专业领域，既可用做本科生的教材，又可作为工程技术人员的技术参考书。

我觉得这套丛书的特点是内容全面、技术新颖、理论联系实际，努力反映信息安全领域的新成果和新技术。在我国信息安全专业人才培养刚刚起步的今天，这套丛

书的出版是非常及时的和十分有益的。

我代表编委会对丛书的作者和广大读者表示感谢。欢迎广大读者提出宝贵意见，以使丛书能够进一步修改完善。

中国工程院院士，武汉大学兼职教授



2003 年 7 月 28 日

前言

21世纪是信息的时代，信息成为一种重要的战略资源，信息技术改变着人们的生活和工作方式，信息产业成为新的经济增长点。信息的安全保障能力成为一个国家综合国力的重要组成部分。信息安全事关国家安全，事关民族兴衰，事关经济发展，必须采取措施确保信息安全。

如何提高我国的信息安全建设水平和加强网络安全的防范意识，已成为全社会共同关注的问题，为适应这一形势，2001年经教育部批准，武汉大学创建了全国第一个信息安全本科专业。2003年经国务院学位办批准，创建了信息安全博士点，2003年经武汉大学批准，创建了信息安全硕士点。武汉大学已经在信息安全领域健全了博士后、博士、硕士和本科培养的教育体系，以期为国家培养更多精通信息安全技术的专业人才。为了加深本科生对信息安全知识的了解，进一步培养在信息安全方面的动手能力和感性认识，武汉大学计算机学院组织编写了这本信息安全综合实验教程。本书是作者在武汉大学计算机学院长期从事信息安全教学和科研的基础上写成的。该书的初稿及讲义已经由2005届信息安全本科教学试用，反映尚好。

本书是对应武汉大学出版社出版的“信息安全技术与教材系列丛书”的配套实验教程。全书共分13章，本书主要内容包括FPGA实验、DSP实验、指纹识别、计算机电磁干扰测试、智能卡实验、Cisco网管软件、计算机病毒、VPN密码机、隔离网闸、IDS、Firewall、数字水印与软件水印、网络攻防实验。

赵波编写第一、二章，刘树波编写第三章，张小武编写第四章，涂航编写第五章，张沪寅编写第七章，傅建明编写第六章，崔竟松编写第八、九章，唐明编写第十章，张文涛编写第十一章，王丽娜编写第十二章，彭国军编写第十三章。张焕国、王丽娜总体指导、设计及审校。

需要声明的是，编写本书的目的是希望帮助读者全面了解信息安全方面的基本技术，以期建立起信息安全方面的防范意识，决不是为怀有不良动机的人提供技术支持，也不承担因为技术滥用而产生的连带责任。

作者收集整理了大量资料，结合自己的研究工作，撰写了本书。由于资料来源的广泛性，书中引用的很多资料没有一一注明出处，对此，在此声明原文版权属于原作者，同时对原作者表示感谢。

由于作者水平有限，不足之处恳请广大读者批评指正。作者衷心感谢给予指导、支持和帮助的所有领导、专家和同行。

作　者

2005年7月

目　录

第一章 FPGA 实验

1.1 绪 论

1.1.1 FPGA/CPLD CAD 技术概述

当今社会是数字化的社会,数字集成电路得到广泛应用。数字集成电路本身在不断地进行更新换代。它由早期的电子管、晶体管、小中规模集成电路,发展到超大规模集成电路以及许多具有特定功能的专用集成电路。但是,随着微电子技术的发展,设计与制造集成电路的任务已不完全由半导体厂商来独立承担。系统设计师们更愿意自己设计专用集成电路(ASIC)芯片,而且希望 ASIC 的设计周期尽可能短,最好是在实验室里就能设计出合适的 ASIC 芯片,并且立即投入实际应用中,因而出现了现场可编程逻辑器件(FPLD),其中应用最广泛的是 FPGA 和 CPLD。

CPLD 是可编程逻辑器件(Complex Programable Logic Device)的简称,FPGA 是现场可编程门阵列(Field Programable Gate Array)的简称,两者的功能基本相同,编程等过程也基本相同,只是芯片内部的实现原理和结构略有不同,所以对初学者,可以忽略这两者的区别,统称为可编程逻辑器件或 CPLD/FPGA 或 PLD。

同以往的 PAL、GAL 等相比较,FPGA/CPLD 的规模比较大,适合于时序、组合等逻辑电路应用场合,它可以替代几十甚至上百块通用 IC 芯片。这样的 FPGA/CPLD 实际上就是一个子系统部件。这种芯片具有可编程性和实现方案容易改动的特点。由于芯片内部硬件连接关系的描述可以存放在磁盘、ROM、PROM 或 EPROM 中,因而在可编程门阵列芯片及外围电路保持不变的情况下,换一块 EPROM 芯片,就能实现一种新的功能。FPGA 芯片及其开发系统问世不久,就受到世界范围内电子工程设计人员的广泛关注和普遍欢迎。

尽管 FPGA、CPLD 和其他类型 PLD 的结构各有其特点和长处,但概括起来,它们是由三大部分组成的:

- 一个二维的逻辑块阵列,构成了 PLD 器件的逻辑组成核心。
- 输入/输出块。
- 连接逻辑块的互连资源,连线资源由各种长度的连线线段组成,其中也有一些可编程的连接开关,它们用于逻辑块之间、逻辑块与输入/输出块之间的

连接。

本章将根据恒科公司的 FPGA 实验台，具体介绍 FPGA 器件的使用方法和编程技巧。

1.1.2 ASIC 和 FPGA/CPLD 电路设计的一般流程

通常可将设计流程归纳为以下 6 个步骤。

1. 设计输入

设计输入包括使用硬件描述语言 HDL、状态图与原理图输入三种方式。HDL 设计方式是现今设计大规模数字集成电路的良好形式，除 IEEE 标准中 VHDL 与 Verilog HDL 两种形式外，尚有各自 FPGA 厂家推出的专用语言，如 Quartus 下的 AHDL。HDL 语言描述在状态机、控制逻辑、总线功能方面较强，使其描述的电路能在特定综合器作用下以具体硬件单元较好地实现；而原理图输入在顶层设计、数据通路逻辑、手工最优化电路等方面具有图形化强、单元节俭、功能明确等特点，常用方式是以 HDL 语言为主，以原理图为辅，进行混合设计，以便发挥两者各自的特色。

2. 设计综合

综合，就是针对给定的电路实现功能和实现此电路的约束条件，如速度、功耗、成本及电路类型等，通过计算机进行优化处理，获得一个能满足上述要求的电路设计方案。综合的过程也就是设计目标的优化过程，最后获得的结构与综合器的工作性能有关。

3. 仿真验证

从广义上讲，设计验证包括功能与时序仿真和电路验证。仿真是指使用设计软件包对已实现的设计进行完整测试，模拟实际物理环境下的工作情况。前仿真是指仅对逻辑功能进行测试模拟，以了解其实现的功能是否满足原设计的要求，仿真过程没有加入时序信息，不涉及具体器件的硬件特性，如延时特性；而在布局布线后，提取有关的器件延迟、连线延时等时序参数，并在此基础上进行的仿真称为后仿真，它是接近真实器件运行的仿真。

4. 设计实现

实现可理解为利用实现工具把逻辑映射到目标器件结构的资源中，决定逻辑的最佳布局，选择逻辑与输入/输出功能连接的布线通道进行连线，并产生相应文件（如配置文件与相关报告）。通常可分为如下五个步骤：

（1）转换：将多个设计文件进行转换并合并到一个设计库文件中。

（2）映射：将网表中逻辑门映射成物理元素，即把逻辑设计分割到构成可编程逻辑阵列内的可配置逻辑块与输入/输出块及其他资源中的过程。

（3）布局与布线：布局是指从映射取出定义的逻辑和输入/输出块，并把它们分配到 FPGA 内部的物理位置。

(4)时序提取:产生一反标文件,供给后续的时序仿真使用。

(5)配置:产生 FPGA 配置时需要的位流文件。

5. 时序分析

在设计实现过程中,在映射后需要对一个设计的实际功能块的延时和估计的布线延时进行时序分析;而在布局布线后,也要对实际布局布线的功能块延时和实际布线延时进行静态时序分析。与综合过程相似,静态时序分析也是一个重复的过程,它与布局布线步骤紧密相联,这个操作通常要进行多次,直到时序约束得到很好的满足。

6. 下载验证

下载是在功能仿真与时序仿真正确的前提下,将综合后形成的位流下载到具体的 FPGA 芯片中,也叫芯片配置。FPGA 设计有两种配置形式:直接由计算机经过专用下载电缆进行配置;由外围配置芯片进行上电时自动配置。因 FPGA 具有掉电信息丢失的性质,因此可在验证初期使用电缆直接下载位流,如有必要再将其烧录到配置芯片中(如 Xilinx 的 XC18V 系列,Altera 的 EPC2 系列)。使用电缆下载时有多种下载方式,如对 Xilinx 公司的 FPGA 下载可以使用 JTAG Programmer、Hardware Programmer、PROM Programmer 三种方式,而对 Altera 公司的 FPGA 可以选择 JTAG 方式或 Passive Serial 方式。因 FPGA 大多支持 IEEE 的 JTAG 标准,所以使用芯片上的 JTAG 口是常用下载方式。

将位流文件下载到 FPGA 器件内部后进行实际器件的物理测试即为电路验证,当得到正确的验证结果后就证明了设计的正确性。电路验证对 FPGA 投片生产具有较大意义。

1.2 MAX + plus Ⅱ 的使用

Altera 公司的 MAX + plus Ⅱ 开发系统是一个完全集成化、易学易用的可编程逻辑设计环境,它可以在多种平台上运用。它所提供的灵活性和高效性是无可比拟的。其丰富的图形界面,辅之以完整的、可以及时访问的在线文档,使学生能够轻松掌握和使用 MAX + plus Ⅱ 软件。MAX + plus Ⅱ 软件支持各种 HDL 设计输入选项,包括 VHDL、VerilogHDL 和 Altera 自己的硬件描述语言 AHDL,它允许设计人员添加自己认为有价值的宏函数。MAX + plus Ⅱ 系统的核心 Compiler 支持 Altera 公司的 FLEX10K、FLEX8000、FLEX6000、MAX9000、MAX7000、MAX5000 和 Classic 可编程逻辑器件系列,提供了商业界惟一真正与结构无关的可编程逻辑设计环境。MAX + plus Ⅱ 的编译器还提供了强大的逻辑综合与优化功能,使用户比较容易地将设计集成到器件中。本节中,首先用最简单的实例向读者展示使用 MAX + plus Ⅱ 软件的全过程。对于该软件的安装和获取,本章不予介绍。

本节将根据软件的特点,着重讲述使用原理图编辑、文本编辑、波形编辑的方法