

<<现代密码算法工程>>

图书基本信息

书名：<<现代密码算法工程>>

13位ISBN编号：9787302278177

10位ISBN编号：7302278172

出版时间：2012-6

出版时间：清华大学出版社

作者：董秀则 等著

页数：252

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<现代密码算法工程>>

内容概要

《普通高等教育“十一五”国家级规划教材·高等院校信息安全专业系列教材：现代密码算法工程》主要涉及密码算法的FPGA硬件实现、软件实现以及密码芯片的安全性设计。内容包括信息安全与密码技术的背景知识；FPGA设计基础知识；各种常用密码算法的FPGA工程实现，书中给出这些密码算法的实现举例和主要程序代码；密码算法的软件实现方法和实现举例；密码芯片的安全性设计等。

本书可作为密码学、信息安全、电子信息工程、通信工程、计算机科学与技术等相关专业本科生的教材或参考书，也可供密码与信息安全研究人员和工程技术人员参考。

<<现代密码算法工程>>

作者简介

路而红，北京电子科技学院教授，毕业于清华大学，首批北京市高等学校教学名师，享受国务院政府特殊津贴。

在高校长期从事电子技术教学与科研工作。

主持多项科研项目并获部级科技进步奖。

主讲的“EDA技术”课程被评为北京市精品课程。

主编的多部教材先后被评为北京高等教育精品教材、普通高等教育“十一五”国家级规划教材，并获得北京市教学成果奖。

<<现代密码算法工程>>

书籍目录

第1章 密码算法工程基础1.1 信息安全与密码技术1.1.1 信息安全概述1.1.2 密码学概述1.2 现代密码技术1.2.1 密码编码与密码分析1.2.2 分组密码与序列密码1.2.3 私钥密码与公钥密码1.3 密码算法工程基础1.3.1 密码算法的硬件实现1.3.2 密码算法的软件实现1.3.3 信息安全系统举例习题1第2章 FPGA原理及应用2.1 FPGA器件原理2.1.1 FPGA框架结构2.1.2 Cyclone器件结构2.1.3 FPGA器件编程2.2 FPGA器件选择2.3 FPGA开发工具2.4 Quartus 使用样例2.4.1 设计输入2.4.2 设计处理2.4.3 波形仿真2.4.4 器件编程2.4.5 原理图文件2.4.6 参数化模块库2.4.7 层次化设计习题2第3章 VHDL语言3.1 VHDL概述3.1.1 VHDL程序结构3.1.2 VHDL语法规则3.2 VHDL并行语句3.2.1 信号赋值语句3.2.2 process语句3.2.3 block语句3.2.4 component语句3.2.5 generate语句3.3 VHDL顺序语句3.3.1 变量赋值语句3.3.2 if语句3.3.3 case语句3.3.4 loop语句3.3.5 null语句3.4 程序包与子程序3.4.1 程序包3.4.2 过程3.4.3 函数3.5 VHDL应用举例3.5.1 求补电路设计3.5.2 双向总线缓冲器设计3.5.3 移位寄存器设计3.5.4 计数器设计3.5.5 有限状态机设计3.5.6 存储器设计习题3第4章 序列密码算法工程实现4.1 序列密码概述4.1.1 序列密码原理4.1.2 序列密码分类4.2 线性密钥序列生成器的工程实现4.2.1 线性反馈移位寄存器4.2.2 线性移位寄存器序列生成器4.3 非线性密钥序列生成器的工程实现4.3.1 非线性移位寄存器序列.....第5章 分组密码算法工程实现第6章 AES算法工程实现第7章 HASH算法工程实现第8章 椭圆曲线点乘算法工程实现第9章 密码算法的软件工程实现第10章 密码芯片安全设计参考文献

<<现代密码算法工程>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>