网络空间安全系列教材
普通高等教育“十三五”规划教材

典型密码算法FPGA实现

◎ 杨亚涛　李子臣　编著

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网络空间安全系列教材
普通高等教育“十三五”规划教材

典型密码算法 FPGA 实现

杨亚涛　李子臣　编著

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

内 容 简 介

本书用 FPGA 实现的密码算法主要分为四大部分，分别是分组密码、公钥密码、Hash 算法和数字签名算法，其中分组密码包括 DES、AES 和 SM4 算法；公钥算法包括 RSA 公钥密码算法、ECC 密码算法和 SM2 密码算法；Hash 算法包括 SHA-1 算法、SHA-3 算法和 SM3 算法；数字签名算法包括 ECC 签名算法和 DSA 签名算法。

本书在 Xilinx 公司的 ISE 平台和 Mentor 公司 ModelSim 仿真软件上编程实现了这些算法，并且还附加了相关实现截图以及密码算法实现效率分析。

本书不仅可作为大学密码与信息安全相关专业本科生以及研究生的教学与参考用书，也可以作为密码与信息安全科研或工程开发人员的参考书。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

典型密码算法 FPGA 实现 / 杨亚涛，李子臣编著. —北京：电子工业出版社，2017.1

ISBN 978-7-121-30383-8

I. ①典… II. ①杨…②李… III. ①密码算法－可编程序逻辑器件－系统设计 IV. ①TN918.1②TP332.1

中国版本图书馆 CIP 数据核字（2016）第 277861 号

策划编辑：戴晨辰
责任编辑：戴晨辰　　文字编辑：刘　芳
印　　刷：三河市双峰印刷装订有限公司
装　　订：三河市双峰印刷装订有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编：100036
开　　本：787×1 092　1/16　印张：13　字数：332.8 千字
版　　次：2017 年 1 月第 1 版
印　　次：2017 年 1 月第 1 次印刷
定　　价：38.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：dcc@phei.com.cn，192910558（QQ 群）。

网络空间安全系列教材

编委会名单

编 委 会 主 任　杨义先

编委会副主任　李子臣　马春光　郑　东

编 委 会 委 员（以汉字笔画为序）

王景中　刘吉强　汤永利

许春根　吴志军　张卫东

杨亚涛　谷大武　辛　阳

罗　平　赵泽茂　贾春福

高　博　彭长根　蒋文保

韩益亮　蔡永泉　蔡满春

编 委 会 秘 书　岳　桢

序

随着经济全球化和信息化的发展，以互联网为平台的信息基础设施，对整个社会的正常运行和发展正起着关键的作用。甚至，像电力、能源、交通等传统基础设施的运行，也逐渐依赖互联网和相关的信息系统才能正常运行。网络信息对社会发展有重要的支撑作用。

网络空间是利用全球互联网和计算系统进行通信、控制和信息共享的动态虚拟空间，包括四个要素，分别是网络平台、用户虚拟角色、资产数据和管理活动，是社会有机运行的神经系统，已经成为继陆、海、空、天之后的第五空间。

网络空间面临的威胁也与日俱增。从国际上看，国家或地区在政治、经济、军事等各领域的冲突都会反映到网络空间中，而由于网络空间边界不明确、资源分配不均衡，导致网络空间的争夺异常复杂。另外，网络犯罪和网络攻击也对个人和企业构成严重威胁。在网络中，个人隐私信息泄露并大范围传播的事件已经屡见不鲜，以非法牟利为目的、利用计算机网络进行的犯罪已经形成了黑色的地下经济产业链。如何充分利用互联网对经济发展的推动作用、保护公民和企业的合法权益，同时又要控制其对经济社会发展带来的负面威胁，需要研究和探索更加科学合理的网络空间安全治理模式。正如习近平总书记所言：“没有网络安全，就没有国家安全”。

加强网络空间安全已经成为国家安全战略的重要组成部分。2014 年 2 月，中央网络安全和信息化领导小组成立。2015 年 6 月，国务院学位委员会、教育部决定在“工学”门类下增设“网络空间安全”一级学科，并明确指出需加强“网络空间安全”的学科建设，做好人才培养工作。2016 年 3 月，国务院学位委员会下发通知，明确全国共有 29 所高校获得我国首批网络空间安全一级学科博士学位授权点。6 月，中央网络安全和信息化领导小组办公室、国家发展和改革委员会、教育部、科学技术部、工业和信息化部、人力资源和社会保障部联合发文，《关于加强网络安全学科建设和人才培养的意见》（中网办发文[2016]4 号）指出，网络空间的竞争，归根结底是人才竞争。我国网络空间安全人才还存在数量缺口较大、能力素质不高、结构不尽合理等问题，与维护国家网络安全、建设网络强国的要求不相适应。提出要加快网络安全学科专业和院系建设；创新网络安全人才培养机制；加强网络安全教材建设；强化网络安全师资队伍建设；完善网络安全人才培养配套措施等意见。

网络空间安全主要研究网络空间中的安全威胁和防护问题，即在有敌手的对抗环境下，研究信息在产生、传输、存储、处理、销毁等各个环节中所面临的威胁和防御措施，以及网络和系统本身面临的安全漏洞和防护机制，不仅仅包括传统信息安全所研究的信息的保密性、完整性和可用性，同时还包括构成网络空间基础设施的安全和可信。从宏观层面来看，网络空间安全的研究对象主要包括：全球各类各级信息基础设施的安全威胁；从微观来看，主要对象包括：通信网络、计算机网络及其设备和应用系统中的安全威胁。

数学、信息论、计算复杂性理论等是网络空间安全所依靠的重要理论基础。

网络空间安全的理论体系由三部分组成。一是基础理论体系，主要包括：网络空间理论、密码学、离散结构理论和计算复杂性理论等；其中，信息的机密性、完整性、可控性、可靠

此为试读，需要完整PDF请访问：www.ertongbook.com

性等是核心，对称加密、公钥加密、密码分析、侧信道分析等是重点，在复杂环境中的可证安全、可信可控及定量分析理论是关键。二是技术理论体系，主要包括网络空间安全保障理论体系，从系统和网络角度，研究和设计网络空间的各种安全保护方法和技术。重点包括：芯片安全、操作系统安全、数据库安全、中间件安全、恶意代码等，从预警、保护、检测到恢复响应的安全保障技术理论。从网络安全角度，以通信基础设施、互联网基础设施等为研究对象，聚焦研究通信安全、网络安全、网络对抗等。三是应用理论体系，从应用角度来看，针对各种应用系统，研究在实际环境中面临的各种安全问题，如 Web 安全、内容安全、垃圾信息等，涵盖电子商务、电子政务、物联网、云计算、大数据等诸多应用领域。

网络空间安全有如下五个研究方向。一是网络空间安全基础，包括：网络空间安全数学理论、网络空间安全体系结构、网络空间安全数据分析、网络空间博弈理论、网络空间安全治理与策略、网络空间安全标准与评测等。二是密码学及应用，包括：对称密码设计与分析、公钥密码设计与分析、安全协议设计与分析、侧信道分析与防护、量子密码与新型密码等。三是系统安全，包括：芯片安全、系统软件安全、虚拟化计算平台安全、恶意代码分析与防护等。四是网络安全，包括：通信基础设施及物理环境安全、互联网基础设施安全、网络安全管理、网络安全防护与主动防御（攻防与对抗）、端到端的安全通信等。五是应用安全，包括：关键应用系统安全、社会网络安全（包括内容安全）、隐私保护、工控系统与物联网安全、先进计算安全等。

中国密码学会教育与科普工作委员会与电子工业出版社合作，共同筹划了这套“网络空间安全系列教材”，主要包括《密码学》、《密码学实验教程》、《公钥密码学》、《应用密码学》、《密码学数学基础》、《密码基础算法》、《典型密码算法 FPGA 实现》、《典型密码算法 JAVA 实现》、《公钥密码算法 C 语言实现》、《密码分析学》、《网络空间安全导论》、《信息安全管理》、《信息系统安全》、《网络空间安全技术》、《网络空间安全实验教程》、《网络攻防技术》、《同态密码学》、《对称密码学》等。希望为信息安全、网络空间安全、网络安全与执法、信息对抗技术等本科专业提供教材，也为密码学、网络空间安全、信息安全等专业的研究生和博士生，以及从事该领域的科研人员提供教材和参考书。为我国网络空间安全教材建设、普及密码知识和网络空间安全人才培养，贡献绵薄之力。

2016 年 12 月

前　言

信息在社会中的地位和作用越来越重要，已成为社会发展的重要战略资源，随之而产生的信息安全问题也日益受到人们的关注，保证信息的安全是保障国家稳定、促进经济发展的重要因素。为了提高我国信息安全的建设水平，提升大学生对密码学与信息安全相关知识的掌握程度和运用能力，国内许多高校开设了不少有关密码学和信息安全的课程，但是所用教材与参考书籍大多侧重于密码算法理论与原理的描述与分析，缺乏对算法的实现过程与实现环境的具体描述，对算法代码的硬件实现更少提及。许多学生学习起来感觉比较茫然和枯燥，以致最后对密码算法的掌握不够深入扎实，对密码学相关知识的学习效果不够理想。因此，本着帮助读者学习、研究密码算法的初衷，本书主要描述典型密码算法的 FPGA 实现过程，侧重培养读者的编程能力，在前人工作的基础上，根据国家公布的有关标准密码算法以及密码学研究的热点，就现行的主要密码算法进行了编程实现。

本书内容丰富、特色鲜明、实用性强，不仅给出了算法的理论知识，还在 Xilinx 公司的 ISE 平台和 Mentor 公司 ModelSim 仿真软件上编程实现了整个算法，并且还附加了相关实现截图以及密码算法实现效率分析。本书不仅可以作为大学本科生以及研究生的教学与参考用书，也可以作为密码科学研究者与工程开发人员的参考书。

本书密码算法主要分四大部分，分别是分组密码、公钥密码、Hash 算法和数字签名算法，其中分组密码有 DES、AES 和 SM4 算法，公钥算法有 RSA 公钥密码算法、ECC 密码算法和 SM2 密码算法，Hash 算法有 SHA-1 算法、SHA-3 算法和我国商密算法 SM3，数字签名算法有 ECC 签名算法和 DSA 签名算法。

本书各章程序实现的参考源代码可以通过华信教育资源网 http://www.hxedu.com.cn 注册免费下载。

全书由杨亚涛博士、李子臣教授负责编著，本书的编写得到了北京电子科技学院相关领导和师生的无私帮助，在此向所有为本书做出贡献的老师和同学们致以衷心的感谢！电子工业出版社为本书的校对、编辑和出版做了大量的工作，对他们也表示诚挚的感谢！

由于时间仓促以及作者水平有限，虽然尽全力对本书进行了校对和检错，但是不免还有疏漏之处，恳请广大读者批评指正。

作　者

2016 年 12 月

目　录

此为试读,需要完整PDF请访问: www.ertongbook.com

第 1 章　密码算法 FPGA 实现基础

1.1 FPGA 概述

目前市场上的 FPGA 芯片主要来自 Xilinx 公司和 Altera 公司，这两家公司占据了 FPGA 80%以上的市场份额，是 FPGA 的主流厂商。除此之外，还有 Actel、Lattice、Atmel 等公司生产相关功能的 FPGA 芯片。

Xilinx（赛灵思）是全球领先的可编程逻辑完整解决方案的供应商，它研发、制造并销售成系列的高级集成电路、软件设计工具以及作为预定义系统级功能的 IP（Intellectual Property）核。客户使用 Xilinx 及其合作伙伴的自动化软件工具和 IP 核对器件进行编程，从而完成特定的逻辑操作。Xilinx 公司成立于 1984 年，首创了现场可编程逻辑阵列（Field Programmable Gate Array，FPGA）这一创新性的技术，并于 1985 年首次推出商业化产品。目前 Xilinx 满足了全世界对 FPGA 产品一半以上的需求，Xilinx 的主流 FPGA 分为两大类：一种侧重低成本应用，容量中等，性能可以满足一般的逻辑设计要求，如 Spartan 系列；还有一种侧重于高性能应用，容量大，性能能满足各类高端应用，如 Virtex 系列。用户可以根据自己实际应用的需求进行选择，在性能可以满足的情况下，优先选择低成本器件。

自 20 世纪 80 年代发明世界上第一个可编程逻辑器件开始，Altera 公司一直秉承着创新的传统，成为世界上“可编程芯片系统”（System on a Programmable Chip，SOPC）解决方案倡导者。Altera 结合带有软件工具的可编程逻辑技术、知识产权（IP）和技术服务，在世界范围内为 14000 多个客户提供过高质量的可编程解决方案。产品系列将可编程逻辑的内在优势（灵活性）、产品及时升级和集成化结合在一起，可以满足客户的不同需求。

Actel 公司成立于 1985 年，位于美国纽约。之前的 20 多年里，Actel 一直效力于美国军工和航空，且被禁止对外出售产品。后来开始逐渐转向民用和商用，出售的产品除了反熔丝系列外，还推出了可重复擦除的 ProASIC3 系列。

Lattice 半导体公司也提供业界成系列的现场可编程门阵列（FPGA）、可编程逻辑器件（Programmable Logic Device，PLD）及其相关软件，包括现场可编程系统芯片（Field Programmable System Chip，FPSC）、复杂的可编程逻辑器件（Complex Programmable Logic Device，CPLD），可编程混合信号产品和可编程数字互连器件。FPGA 和 PLD 是广泛使用的半导体元件，最终用户可以将其配置成特定的逻辑电路，从而缩短设计周期，降低开发成本。

Atmel 公司是世界上高级半导体产品设计、制造和营销的领先者，推出的产品包括微处理器、可编程逻辑器件、非易失性存储器、安全芯片、混合信号及 RF 射频集成电路等。

1.1.1 Xilinx 公司的代表芯片

1. 面向高性能的 Virtex-5 FPGA 系列

系统集成平台——Virtex-5 系列 FPGA 提供了 4 种新型平台，每种平台都在高性能逻辑、串行连接、信号处理和嵌入式处理性能方面实现了最佳平衡。

常用的 3 款平台特性如下。

（1）Virtex-5 LX 平台：针对高性能逻辑进行了优化。

（2）Virtex-5 LXT 平台：针对带有低功耗串行连接功能的高性能逻辑进行了优化。

（3）Virtex-5 SXT 平台：针对带有低功耗串行连接功能的 DSP 和存储器密集型应用进行了优化。

2. 面向低成本的 Spartan-3 FPGA 系列

90nm Spartan-3 系列 FPGA 的发售量已经超过 3 000 万片，它是业内首款大容量 FPGA 系列产品，针对多个特定领域进行了平台优化。

（1）面向数字信号处理的 Spartan-3A DSP 平台。这个平台对 DSP 进行了优化，适合那些需要集成 DSP MAC 和扩展存储器的应用，特别适合那些需要低成本 FPGA 来实现信号处理（如军用无线电、监视照相机、医学成像等）的应用设计。

（2）面向非易失性应用的 Spartan-3AN 平台。这个平台主要针对非易失性、系统集成、安全、大型用户 Flash 的应用，特别适用于低成本嵌入式控制器。

（3）面向主流应用的 Spartan-3 平台。

① Spartan-3A 平台：针对 I/O 进行了优化。这个平台主要应用在对 I/O 数目和性能比要求较高的场合，特别适于桥接、差分信号和存储器接口等需要宽接口或者多个接口以及一定处理能力的应用。

② Spartan-3E 平台：针对逻辑进行了优化。这个平台主要应用在对逻辑密度要求较高的场合，特别适于逻辑集成、DSP 协处理和嵌入式控制等这些需要进行大量处理和窄接口或者少量接口的应用。

③ Spartan-3 平台：这个平台主要针对那些高逻辑密度和高 I/O 数目的应用，特别适用于高度集成的数据处理应用。

1.1.2 Altera 公司的代表芯片

1. 面向高性能的 Stratix III FPGA 系列

与 Xilinx 的 Virtex-4 系列对应，Altera 公司推出了 Stratix III 系列 FPGA 体系结构。Stratix III 系列不仅性能比上一代提高很多，更重要的是静态和动态功耗比前代 FPGA 降低了 50%。Stratix III 器件经过设计，支持高速内核以及高速 I/O，并且具有非常好的信号完整性，例如，它能够实现 400MHz DDR3 的 FPGA。这种性能的提高源于以下几点：增强的 DSP 模块实现了信号处理算法；优化的内部存储器改进了信号存储器接口；高性能的外部存储器接口改进了布线体系结构；灵活的 I/O 支持最新的外部存储器标准。为了给客户的设计应用提供最高性价比的解决方案，Altera Stratix III FPGA 提供了 3 种型号，分别针对逻辑、DSP 和存储器以及收发器进行了优化。

2．面向低成本的 Cyclone III FPGA 系列

低成本的 Cyclone III FPGA 是 Altera Cyclone 系列的第三代产品。Cyclone III FPGA 系列同时实现了低功耗、低成本和高性能，进一步扩展了 FPGA 的应用；Cyclone III FPGA 采用 TSMC 公司的 65-nm 低功耗（LP）工艺技术，Cyclone III 器件对芯片和软件采取了更多的优化措施，在所有 65-nm FPGA 中是功耗最低的，在对成本和功耗敏感的大量应用中，显示出很大的优势。Cyclone III 系列包括 8 个型号，具有 5k 到 120k 个逻辑单元（LE），最多有 534 个 I/O 引脚。Cyclone III 器件具有 4MB 嵌入式存储器、288 个嵌入式 18×18 乘法器、专用外部存储器接口电路、锁相环（PLL）以及高速差分 I/O 等模块。

1.2 FPGA 工作原理

FPGA 是基于 PAL（Programmable Array Logic）、GAL（General Array Logic）、CPLD 等开发出来的新技术，常作为专用集成电路控制的分电路，如图 1.1 所示，在原有可编程控制器中进行了优化调整。FPGA 采用了逻辑单元阵列这样一个概念，内部包括可配置逻辑模块、输出输入模块和内部连线三个部分。FPGA 利用小型查找表（16x1RAM）来实现组合逻辑，每个查找表连接到一个 D 触发器的输入端，触发器再来驱动其他逻辑电路或驱动 I/O，由此构成了既可实现组合逻辑功能又可实现时序逻辑功能的基本逻辑单元模块。

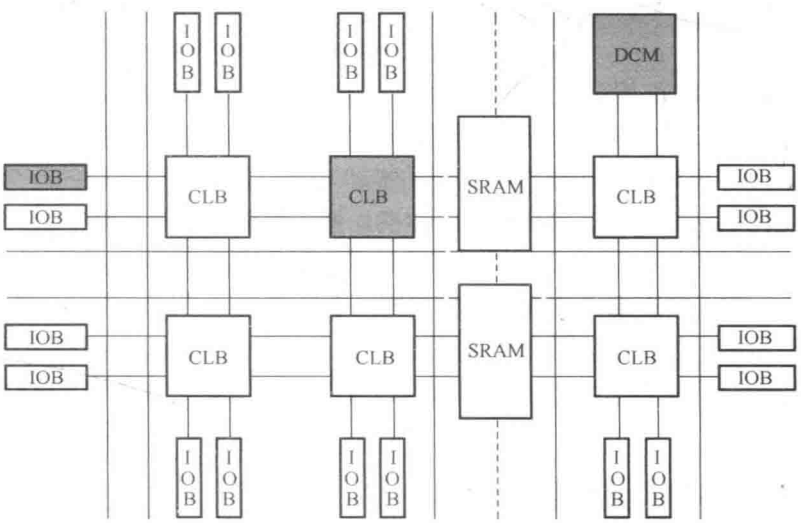

图 1.1　FPGA 内部结构

FPGA 结构模块的功能描述如下。

BRAM（Bipolar Random Access Memory）模块：专用集成电路是服务于各个行业控制的应用型电路，FPGA 在结构模块布局方而也要适应实际操作的要求。一般情况下，FPGA 配备了专用的内嵌式随机存储器（RAM）来针对数据端口的传输位置、存储结构、元件功能等要素，提供一个稳定的逻辑存储方式。以内存储操作为例，FPGA 搜索到某个触发器时，要准确地感应出电路中动态或静态存储方式，再由 BRAM 辅助存储器作为电路信号收录装置。

DCM（Data Control Memory）模块：FPGA 的逻辑是通过向内部静态存储单元加载编程

数据来实现的，业内大多数 FPGA 均提供数字时钟管理。先进的 FPGA 不仅提供数字时钟管理，还提供相位环路锁定，相位环路锁定能够提供精确的时钟综合，并实现过滤功能。数字控制模块（DCM）的主要作用是对门电路各程序指令进行规划，限定数据信号传输的标准位置，避免数据冗杂从而提升电子系统控制的效率。另外，数字控制模块也对门电路运行时间进行精确控制，防止信号延迟而造成电子仪器的误动作。

CLB（Configurable Logic Block）模块：逻辑处理是 FPGA 中处理数据的有序流程，按照电路信号编码程序的规则对门电路进行优化编程。可配置逻辑块（CLB）的实际数量和特性会根据器件的不同而不同，但每个 CLB 都包含一个可配置的开关矩阵，此矩阵由 4 或 6 个输入以及一些选型电路和触发器组成。

IOB（Input Output Block）模块：可编程输入输出单元（IOB）是现场可编程门阵列的基本构造，输入/输出（I/O）模块负责 FPGA 数据信号收录、传输作业要求等。从结构层次来划分，IOB 模块是芯片与外界电路的接口部分，完成不同电气特性下对输入/输出信号的驱动与匹配要求。I/O 接口由多个单元组成，按照电路的相位、电阻、元控件等指标，严格控制门电路的运作流程。

总之，FPGA 是基于 SRAM 的可编程器件，它以功能很强的 CLB 为基本逻辑单元，可以实现各种复杂的逻辑功能，FPGA 还具有可扩展的优点。由于 FPGA 的性能和灵活性，以及新的简明设计和实施方法，在很多新兴应用领域中 FPGA 都成为优选的解决方案。

1.3 FPGA 语法基础

Verilog HDL 和 VHDL 是目前最流行的硬件描述语言，均为 IEEE 标准，被广泛应用于可编程逻辑器件的项目开发。两者都是用于逻辑设计的硬件描述语言，都能形象化地表示电路的行为和结构，支持逻辑设计中层次与范围的描述，可以描述简化电路的行为，具有电路仿真验证机制，支持电路描述由高层到低层的转换，便于管理与设计混用。

但两者又有不同的特点：Verilog HDL 产生较早，容易被接受，学习者如果有 C 语言基础，就能很快掌握它；但是它在系统抽象方面比较弱，不适合大型系统的开发，经过不断的升级，其系统级表述性能和可综合性能得到了大幅度提升。VHDL 需要 Ada 编程语言基础，学习者需要较长时间才能全面掌握它。不过，这两种语言仍处于不断完善当中，都在向更高级描述语言的方向迈进。

1.3.1 Verilog HDL 语法要点

1. 一般的模块结构

module<模块名>（<端口列表>）
<定义>
<模块条目>
endmodule

2. IO 端口种类

Input 表示模块从外界读取数据的接口，在模块内不可写。Output 表示模块往外界送出数据的接口，在模块内不可读。Inout：可读取数据，也可以送出数据。

对相同位宽的输入输出信号可以一起声明，比如，input[3:0] a,b；不同位宽的必须分开写，比如，input [5:0] a; input [6:0] b；内部信号为 reg 类型，内部信号的状态有 0、1、x、z。

3．赋值运算符

逻辑功能描述中，常用 assign 语句来描述组合逻辑电路，always 语句既可以描述组合逻辑电路又可以描述时序逻辑电路，还可以用元件调用方法描述逻辑功能 always 之间、assign 之间和实例引用，它们之间都是并行执行，always 内部是顺序执行。

assign 赋值语句中，被赋值的信号都是 wire 类型。assign 之所以被称为连续赋值，是因为它要不断检测表达式的变化。always 模块里被赋值的信号都要定义为 reg 类型，因为 always 可以反复执行，而 reg 表示信号的寄存，可以保留上次执行的值。

在赋值运算中，阻塞式赋值（=）表示在同一个 always 过程中，后面的赋值语句要等待前一个赋值语句执行完，后面的语句被该赋值语句阻塞。非阻塞式赋值（<=）表示在同一个 always 过程中，非阻塞赋值语句是同时进行的，排在后面的语句不会被该赋值语句所阻塞。块结束后才能完成赋值，块内所有非阻塞式赋值在 always 块结束时同时被赋值。在 always 过程中，begin…end 块内按先后顺序被立即赋值。

4．数据类型

Verilog HDL 的数据类型分为三类：线网类型、寄存器类型和参数类型。线网类型主要表示 Verilog HDL 中结构化元件之间的物理连线，其数值由驱动元件决定，如果没有驱动元件接到线网上，则其默认值为高阻状态 z；寄存器类型主要表示数据的存储单元，其默认值为不定值 x；参数类型常用参数来声明运行时的常数，可以用字符串表示的任何地方都可以用定义的参数来代替，参数是本地的，其定义只在本模块内有效。线网类型和寄存器类型最大的区别在于：寄存器类型数据保持最后一次的赋值，而线网类型数据则需要持续的驱动。

下面对本书常用到的数据类型进行介绍。wire 表示直通，即输入有变化，输出马上无条件地反映（如“与”、“非门”的简单连接）。reg 表示一定要有触发，输出才会反映输入的状态。reg 相当于存储单元，wire 相当于物理连线。reg 表示一定要有触发，没有输入的时候可以保持原来的值，但不直接与实际的硬件电路对应。对于 always 语句而言，赋值要申明成 reg；连续赋值 assign 的时候要用 wire。

5．关系运算符

==和!=这两个运算符只用于比较 0、1，遇到 z 状态或 x 状态时，结果都为 x 状态（x 在 if 中作为假条件）。

===和!==这两个运算符比较苛刻，属于 x 和 z 的精确比较，结果可能是 0、1。

其他关系运算符操作简单，这里就不再叙述。

6．逻辑运算符

&&和||是双目运算符，要求有两个操作数；而！是单目运算符，只要求一个操作数。

7．移位运算符

移位运算时，左移将保留高位，例如 4'b1000<<1 等于 5'b10000；右移则舍弃低位，例如 4'b0011>>1 等于 4'b0001。

8. 跳转语句

if …else 有三种使用形式，如下所示。

使用形式 1：if (<条件表达式>) 语句或语句块；

使用形式 2：if (<条件表达式>) 语句或语句块 1；

else 语句或语句块 2；

使用形式 3：if (<条件表达式 1>) 语句或语句块 1；

else if (<条件表达式 2>) 语句或语句块 2；

……；

else if (<条件表达式 *n*>) 语句或语句块 *n*；

else 语句或语句块 *n*+1。

第三种形式适合描述优先编码器，if 条件中把状态 0/x/z 当成假，状态 1 当成真，非 0 的数值也当成真。

9. 分支语句

case 语句是一个多路条件分支语句，case 语句有三种形式：case（四种状态的比较），casez（忽略 z 状态的比较），casex（忽略 x 和 z 状态的比较，只看哪些位的信号有用）。case 语句中所有表达式值的位宽必须相等。

10. 循环语句

Verilog HDL 中有四种循环语句，包括 for 循环、while 循环、forever 循环、repeat 循环。其语法和用途和 C 语言相似。

11. 语句块

有两种特殊的语句块：begin 顺序语句 ... end ，fork 并行语句... join，其差别在于块内语句的起止时间、执行顺序、相对延时等。块被命名后，因为变量都是静态的，其内部变量都可以被调用。

12. 过程结构

initial 块只被无条件执行一次，always 块在满足条件时可以被不断执行；initial 块常用来写测试文件，always 块常用来进行电路描述，它既可以描述组合逻辑电路又可以描述时序逻辑电路，但如果后面有敏感信号列表则不能用 wait 语句。always 语句既可以描述电平触发又可以描述边沿触发，而 wait 语句只能描述电平触发；assign 常用于描述组合逻辑电路，测试文件中一般都是先用 initial 语句，后用 always 语句。

13. 生成块

生成块的本质是使用循环内的一条语句代替多条重复的 Verilog HDL 语句，以便简化用户的编程。genvar 用于声明生成变量，生成变量只能用在生成块之间。

14. 模块设计

一个模块设计包括 3 个部分：电路模块设计、测试模块设计和设计文档编写。设计者通过布局布线工具来生成具有布线延迟的电路，再进行仿真，得到时序分析报告。从时序分析

此为试读，需要完整PDF请访问：www.ertongbook.com