一种基于 FPGA 的 3DES 加密算法实现

任　芳,杨承睿,陈雷华

陕西省气象科技服务中心,陕西 西安 710014)

摘要 为了满足大量连续数据加解密的要求以及提高加密算法安全性的要求,采用有限状态机和流水线等关键技术,设计并实现了基于 FPGA 的 3DES 加密算法的加密电路. 在 Xilinx Virtex4 系列的 FPGA 平台上采用 ISE 10.1 开发工具实现仿真验证和逻辑综合. 结果表明,3DES 加密系统的加解密速度可以达到 860.660Mb/s,提高了加解密速度,并且有效减少了资源占用率. 最终,系统可广泛应用于网络安全产品及其他安全设备中.

关键词 FPGA 3DES 算法 VHDL 有限状态机 流水线技术

中图分类号 TP309.7　　文献标识码 A

0 引　言

现代分组加密算法[1] 如 DES[2]、3DES[3-4]、AES 既可以用硬件也可以用软件来实现. 软件加密是通过在主机上运行加密软件来实现加密功能,除占用主机资源外,其运算速度较硬件加密要慢,在某些高速数据传输的场合无法满足要求,密钥或以明文方式存储在程序中,或以加密的方式存储在文件或数据库中,重要数据 如个人密码 PIN 等 会在某一时刻以明文形式出现在计算机的内存或磁盘中,安全性也较差. 与传统的软件加密相比,硬件加密是通过独立于主机系统外的硬件加密设备实现的,所有关键数据的存储、运算都在内部通过硬件实现,不占主机资源,速度快,安全性较高,稳定性和兼容性也比较好. 同时,硬件加密是商业和军事用途的主要选择. 许多加密算法采用软件实现效率是很低的,如 DES、3DES、RSA 等,需要用专门的硬件来加以实现.

3DES 168 位密钥 是通过增强其算法复杂性来保障其安全性,同时底层以 DES 算法为基础可以使原系统不作大的改动,然而 3DES 的根本缺点在于用软件实现速度比较慢. 此外,由于 DES、3DES 加密算法经常采用移位、异或、换位等位操作,因此硬件实现更具有其特别的优势. 因而用硬件实现并在硬件平台上优化 3DES 这种比较复杂的算法成为一个新的研究热点.

随着 EDA 技术的成熟,采用 FPGA[5] 现场可编程门阵列 设计数字电路已经成为数字电路系统领域的主要设计方式之一. 在信号的处理和整个系统的控制中,FPGA 不仅能缩减电路的体积,提高电路的稳定性,而且其先进的开发工具使整个系统的设计调试周期大大缩短. FPGA 既继承了 ASIC 的大规模、高集成度、高可靠性的优点,又克服了普通 ASIC 设计周期长、投资大、灵活性差的缺点,逐步成为复杂数字硬件电路设计的理想首选,因此研究和设计 3DES 算法的 FPGA 设计具有现实意义. 本文采用有限状态机和三级流水线等关键技术,以及模块化设计方法最终实现了系统并对系统进行仿真和综合优化,进一步提高

系统的整体性能.

1 DES 和 3DES 算法描述

1.1 DES 算法

DES 自公开以来受到过各种有针对性的攻击，经历了长期的考验，并在此基础上衍生了新的算法，具有很强的应用性. 其整个体制是公开的，系统的安全性完全靠密钥的保密. DES 处理的明文分组和密文分组长度均为 64 位，使用 64 位的密钥，其中有效长度为 56 位.

DES 加密算法的加密流程可概括为初始置换运算、16 轮循环迭代运算、逆初始置换运算 3 个过程. 通过一个初始置换，将明文分成左半部分和右半部分，然后进行 16 轮完全相同的运算，最后经过一个末置换便得到 64 位密文. 每一轮的运算包含扩展置换、S 盒代换、P 盒置换和两次异或运算，另外每一轮中还有一个轮密钥（子密钥）.

DES 的解密过程和加密相似，解密时使用与加密同样的算法，不同在于子密钥的使用次序要反过来. 图 1 为 DES 算法加密流程图.

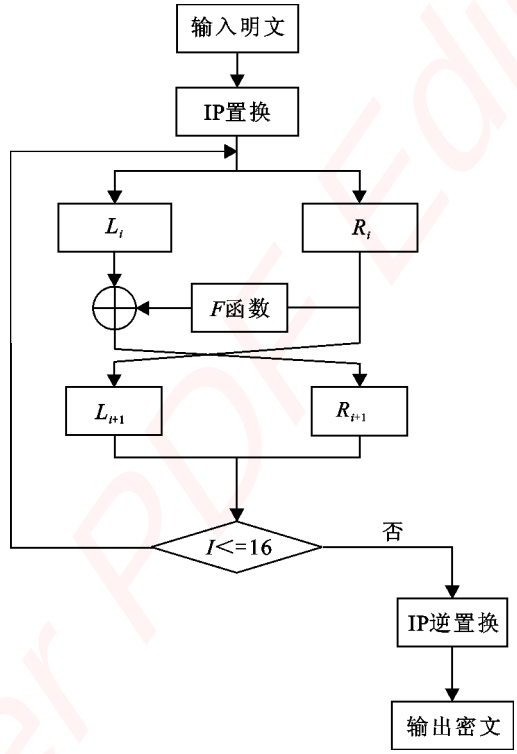

图 1 DES 加密算法流程图

1.2 3DES 算法

三重 DES 算法（Triple-DES、3-DES）是 DES 算法一个更安全的变形. 该加密算法的密钥由 3 个 64 位密钥 K_1，K_2 和 K_3 组成，以一次 DES 加密算法为基本模块，对 64 位明文分组进行加密. 设 $E_K(x)$ 和 $D_K(X)$ 表示用 DES 算法对 64 位的分组数据进行加密和解密，密钥为 K，64 位明文为 X，64 位密文为 C，则加解密过程可以用以下公式表示：

3DES 的加密过程描述公式为 $C = E_{K_3}(D_{K_2}(E_{K_1}(X)))$；

3DES 的解密过程描述公式为 $X = D_{K_1}(E_{K_2}(D_{K_3}(C)))$.

为了获得更高的安全性，3 个密钥应该是互不相同的. 这样，本质上就相当于用一个长为 168 位的密钥进行加密. 对安全性需求不十分高的数据，K_3 可以等于 K_1，在这种情况下，密钥的有效长度为 112 位.

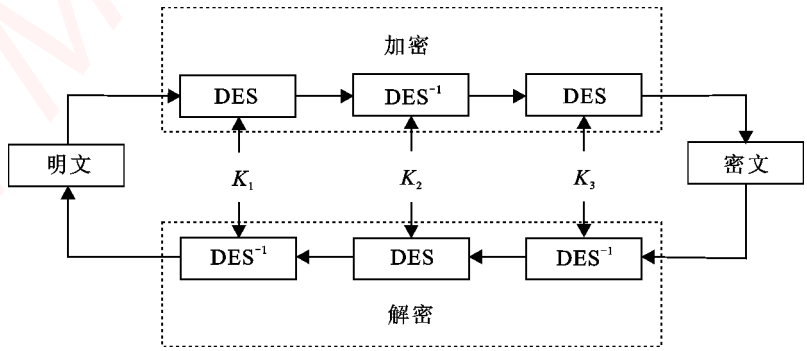

图 2 3DES 加密算法加密和解密流程图

2 FPGA 设计实现

2.1 设计方案

设计的宗旨是在尽可能减少资源消耗的情况下又能提高运算速度. 因此，系统采用有限状态机和三级流水线等关键技术，在合理占用资源的情况下，尽可能提高系统的性能，并对设计后的系统进行综合优化，进一步提高系统处理数据的速度.

根据上述设计目标以及对 3DES 算法的研究分析，采用模块化设计方法构建了 3DES 算法的整体结构. FSM、GETEY、3 个 DES 运算模块形成 3 级流水线结构构成整个 3DES 系统的运算模块. 系统整体结构如图 3 所示. 图 3 中，FSM（有限状态机）负责所有状态转换，是整个电路的控制核心. GETKEY 在控制信号的控制下，实现初始密钥的接收，产生运算模块每次迭代所需要的子密钥并存储. DES_1，DES_2，DES_3 根据状态控制处理进程，完成对数据的加解密的流水操作.

2.2 关键技术

2.2.1 有限状态机的设计 所谓状态机就是事物存在状态的一种综合描述，说明任意两个状态之间的转

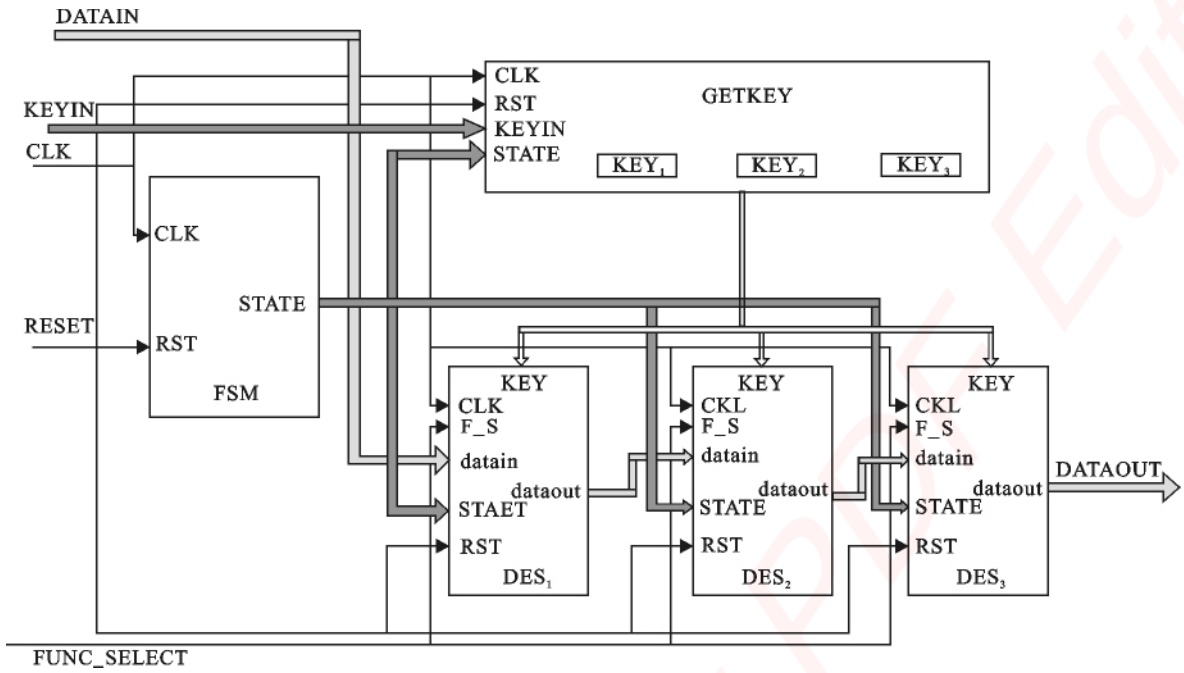

图 3　3DES 加密算系统整体结构图

变条件. 每一个控制步或进程代表一种状态,与每一控制步相关的转移条件决定次态的状态和输出. 其程序结构简单,控制灵活 能有效消除毛刺现象 进程并行执行,能有效提高运算速度 使用完整的容错技术,具有极高的可靠行 生成的硬件电路简单,进而大大节省了硬件资源.

VHDL 主要用于描述数字系统的结构、行为、功能和接口. 其程序结构特点是,将一项工程设计实体 可以是一个元件,一个电路模块或一个系统 分成外部 即端口 或内部. 在对一个设计实体定义了外部界面后,一旦其内部开发完成,其他设计就可以直接调用这个实体. 这种设计实体分成内外部分的概念就是 VHDL 系统设计的基本点. 因此,设计实体可用传统有限状态机模型来描述. 在 VHDL 设计中,可以不需要进行繁琐的状态分配、化简状态方程等步骤,可以简便地定义状态变量,将状态描述成进程,这个进程可以传出信号来控制其他进程,从而实现各种功能. 因此,采用有限状态机 FSM 实现整个加密电路的状态控制.

在初始状态下,有限状态机产生状态信号对密钥输入和明/密文输入进行控制,从而实现对密钥模块和 DES 运算模块的调用. 该状态机共有 2 个状态,即 WaitKeyState 等待密钥输入状态 、WaitDataState 等待明/密文输入状态 .图 4 为系统顶层模块中状态转换图.

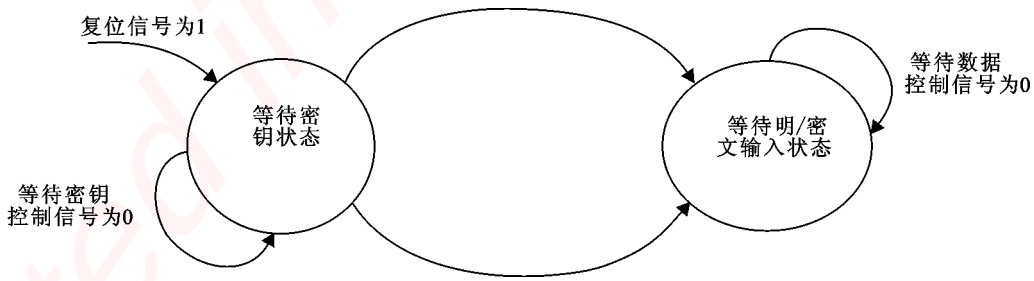

图 4　系统顶层模块中状态转换图

16 个 48 位子密钥完成 16 轮循环运算,其过程复杂,相应控制也难以实现,因此,采用有限状态机设计,完成各个子密钥与相应轮数匹配控制以及数据处理过程控制. 该状态机共设计了 waitkey 等待密钥输入状态 、waitdata 等待明/密文数据输入状态 、initialround 初始轮状态 、reapeatround 重复轮状态 、finalround 最后轮状态 等 5 个状态类型,同时使用一个 4 位计数器 roundcounter 记录轮数. 图 5 为 16 轮运算与其子密钥选择状态转换图.

2.2.2　流水线结构的设计　流水线设计就是将组合逻辑系统地分割,并在各个部分 分级 之间插入寄存器,并暂存中间数据的方法,目的是提高数据吞吐率 提高处理速度 .基于性能和资源占用情况的综合

考虑,采用了 3 级流水形式,每个 DES 作为一级流水. 在每级 DES 中实现 16 轮迭代运算. 设计密钥产生模块提前生成 16 轮迭代所需的子密钥. 并由 FSM 控制 16 轮子密钥与循环迭代次数的匹配. 这样系统从第一个数据块开始加密 或解密 起,经 48 个周期的延迟后,从第 49 个周期开始,以后每 16 个时钟周期后都有一个加解密后的 64 位数据输出.

2.2.3 密钥匙模块的设计 在设计中,密钥生成器的设计是独立于 DES 轮函数运算实现的. 该模块在控制信号的控制下,实现初始密钥的接收,并产生运算模块每次迭代所需要的子密钥功能.

以往设计采用 3 组密钥分时复用一个密钥产生模块,使得系统整体加解密速度不如并行复制多个操作模块的快. 因此,本设计采用并行复制 3 个密钥模块,这样减少了每组密钥分时等待密钥模块的时间和每轮运算等待子密钥的时间.

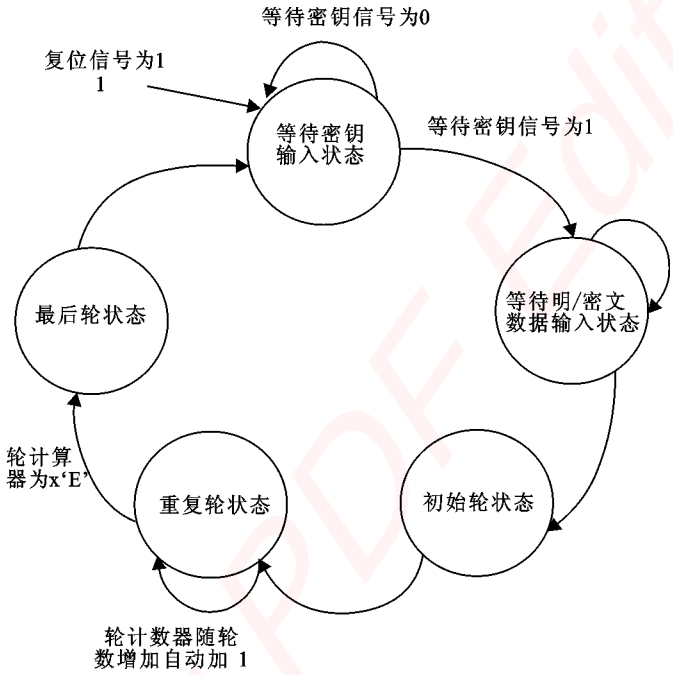

图 5 16 轮运算与其子密钥选择状态转换图

DES 算法的每一个轮次加密或者解密的子密钥皆通过循环左移及循环右移实现,而且每个轮次都有确定的移动位数,可以通过完整的分析推导出每个轮次,每个子密钥对应初始密钥的数值,从而与中间子密钥无关. 因此,本设计的子密钥生成采用直接赋值提前生成的方法,通过用一个计数器来控制轮数,从而选择相应的子密钥. 所有子密钥全部并行同时生成,事先准备好,由子密钥选择信号来选择,送到相应的运算模块中. 通过并行复制 3 个密钥匙模块及各个子密钥提前生成的设计,提高了系统的性能.

3 系统仿真结果

对系统设计完成后,要对系统进行仿真验证,尽可能早发现设计缺陷. 本文的仿真验证采用自底向上的方法,把验证分成模块级仿真和系统级仿真两部分. 篇幅有限,此部分只给出系统级仿真结果图.

为了更直观的从图中看出仿真结果,输 3 个初始密钥都为 ox00 00 00 00 00 00 00 00,data_in [0 63] 输入为 ox80 00 00 00 00 00 00 00,如图 6 所示. 从图 6 中可以看出各种信号以及数据输入情况,对输入明文进行加密操作,在第 49 个周期的时候输出密文. 在图 7 中,当输出信号为真时,输出密文为 ox95 f8 a5 dd 31 d9 00. 仿真结果正确. 验证系统解密操作时,把加密时输出的密文作为解密时的明文,密钥不变,输出结果为加密时的明文,仿真结果同样正确. 图略.

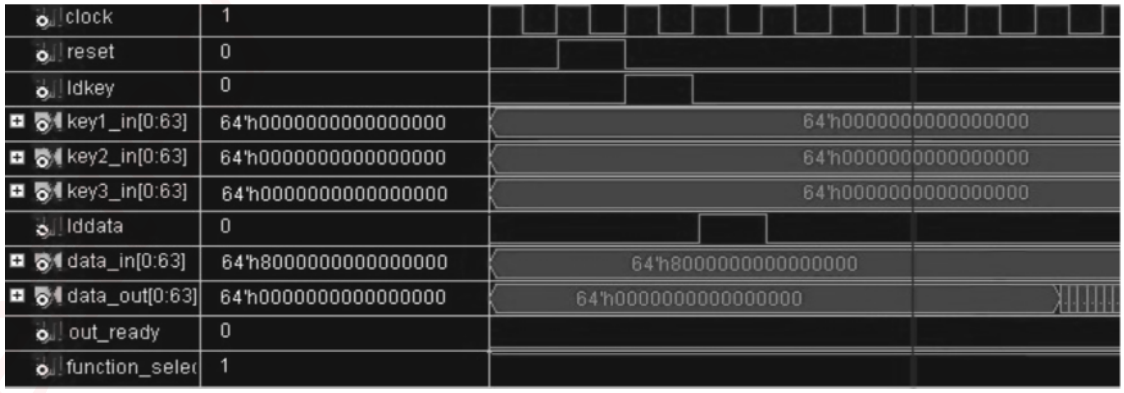

图 6 out_ready 为"0"时 3Des_top 加密仿真波形图

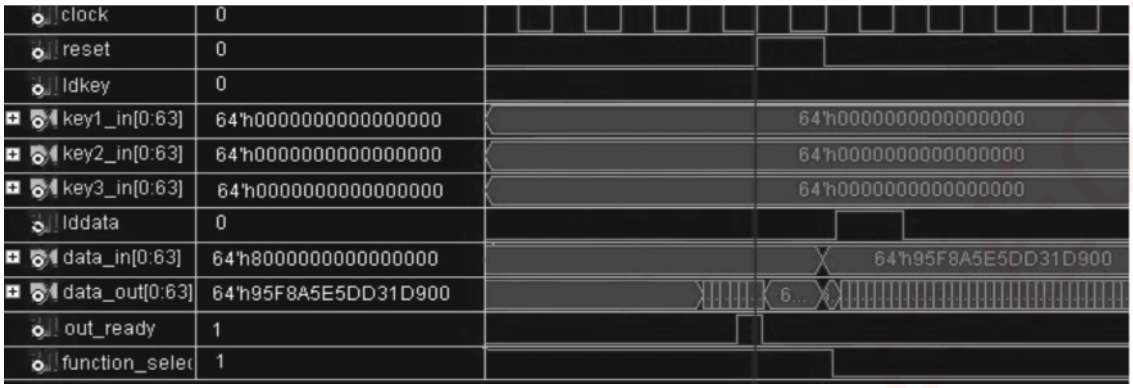

图 7　out _ ready 为“1”时 3Des _ top 加密仿真波形图

4　结束语

此次加密算法的实现主要采用 Xilinx 公司的 Virtex4 系列的 xc4vlx25-12-ff676 器件作为平台，在 ISE10. 1 下对 VHDL 代码进行编译、综合、适配和仿真.

分析综合结果，系统时钟的最高工作频率为 215. 165MHz，最短建立时间为 3. 454ns，最长保持时间为 3. 793ns. 该设计可广泛应用于网络安全产品及其他安全设备中.

参考文献　：

[1]　杨波. 现代密码学 [M]. 北京 清华大学出版社，2003 146 148-149.

[2]　潘文明. DES 加密芯片的研制及实现 [D]. 广州 暨南大学，2008.

[3]　党志军，张国杰. 高速 3 _ DES 算法 IP 核的设计与实现 [D]. 郑州 解放军信息工程大学，2007.

[4]　邵金祥，何志敏. 基于 FPGA 的 3DES 加密算法高速实现 [J]. 现代电子技术 2004，27 2(上)55-57.

[5]　李云松，宋锐，雷杰，杜建超. Xilink FPGA 设计基础 V(HDL 版)M]. 西安　西安电子科技大学出版社，2008.

3DES implementation based on FPGA

REN Fang，YANG Cheng-rui，CHEN Lei-hua

Shaanxi Meteorological Science and Technology Service Center，Xi′an 710014，China)

Abstract　In order to meet the demand of plenty continuous encrypting-deciphering，and meet the demand of enhancing the security of encrypting-deciphering algorithm，the fundamental technologies such as pipeline technology and finite state machine (FSM)are applied，3DES encryption algorithm′s encryption chip′s circuit based on FPGA are designed and realized. On the platform of FPGA of Xilinx Virtex4 series，the ISE 10. 1 development kits is used to realize the simulation confirmation and the logic synthesis. The result indicates that the 3DES cryptographic system′s speed is able to achieve 860. 660Mbps，and the encrypting-deciphering speed is greatly enhanced. The design could be used in network security products and other security equipment extensively.

Key words　3DES；FPGA；VHDL；state machine；pipeline technology

嵌入式资源免费下载

总线协议：

1. 基于 PCIe 驱动程序的数据传输卡 DMA 传输
2. 基于 PCIe 总线协议的设备驱动开发
3. CANopen 协议介绍
4. 基于 PXI 总线 RS422 数据通信卡 WDM 驱动程序设计
5. FPGA 实现 PCIe 总线 DMA 设计
6. PCI Express 协议实现与验证
7. VPX 总线技术及其实现
8. 基于 Xilinx FPGA 的 PCIE 接口实现
9. 基于 PCI 总线的 GPS 授时卡设计
10. 基于 CPCI 标准的 6U 信号处理平台的设计
11. USB30 电路保护
12. USB30 协议分析与框架设计
13. USB 30 中的 CRC 校验原理及实现
14. 基于 CPLD 的 UART 设计
15. IPMI 在 VPX 系统中的应用与设计
16. 基于 CPCI 总线的 PMC 载板设计
17. 基于 VPX 总线的工件台运动控制系统研究与开发
18. PCI Express 流控机制的研究与实现
19. UART16C554 的设计
20. 基于 VPX 的高性能计算机设计
21. 基于 CAN 总线技术的嵌入式网关设计
22. Visual C 串行通讯控件使用方法与技巧的研究
23. IEEE1588 精密时钟同步关键技术研究
24. GPS 信号发生器射频模块的一种实现方案
25. 基于 CPCI 接口的视频采集卡的设计
26. 基于 VPX 的 3U 信号处理平台的设计
27. 基于 PCI Express 总线 1394b 网络传输系统 WDM 驱动设计
28. AT89C52 单片机与 ARINC429 航空总线接口设计
29. 基于 CPCI 总线多 DSP 系统的高速主机接口设计
30. 总线协议中的 CRC 及其在 SATA 通信技术中的应用
31. 基于 FPGA 的 SATA 硬盘加解密控制器设计
32. Modbus 协议在串口通讯中的研究及应用
33. 高可用的磁盘阵列 Cache 的设计和实现
34. RAID 阵列中高速 Cache 管理的优化

35. 一种新的基于 RAID 的 CACHE 技术研究与实现
36. 基于 PCIE-104 总线的高速数据接口设计
37. 基于 VPX 标准的 RapidIO 交换和 Flash 存储模块设计
38. 北斗卫星系统在海洋工程中的应用
39. 北斗卫星系统在远洋船舶上应用的研究
40. 基于 CPCI 总线的红外实时信号处理系统
41. 硬件实现 RAID 与软件实现 RAID 的比较
42. 基于 PCI Express 总线系统的热插拔设计
43. 基于 RAID5 的磁盘阵列 Cache 的研究与实现
44. 基于 PCI 总线的 MPEG2 码流播放卡驱动程序开发
45. 基于磁盘异或引擎的 RAID5 小写性能优化
46. 基于 IEEE1588 的时钟同步技术研究
47. 基于 Davinci 平台的 SD 卡读写优化
48. 基于 PCI 总线的图像处理及传输系统的设计
49. 串口和以太网通信技术在油液在线监测系统中的应用
50. USB30 数据传输协议分析及实现
51. IEEE 1588 协议在工业以太网中的实现
52. 基于 USB30 的设备自定义请求实现方法
53. IEEE1588 协议在网络测控系统中的应用
54. USB30 物理层中弹性缓冲的设计与实现
55. USB30 的高速信息传输瓶颈研究
56. 基于 IPv6 的 UDP 通信的实现
57. 一种基于 IPv6 的流媒体传送方案研究与实现
58. 基于 IPv4-IPv6 双栈的 MODBUS-TCP 协议实现
59. RS485CAN 网关设计与实现
60. MVB 周期信息的实时调度
61. RS485 和 PROFINET 网关设计
62. 基于 IPv6 的 Socket 通信的实现
63. MVB 网络重复器的设计
64. 一种新型 MVB 通信板的探究
65. 具有 MVB 接口的输入输出设备的分析
66. 基于 STM32 的 GSM 模块综合应用
67. 基于 ARM7 的 MVB CAN 网关设计
68. 机车车辆的 MVB CAN 总线网关设计
69. 智能变电站冗余网络中 IEEE1588 协议的应用

VxWorks：

1. 基于 VxWorks 的多任务程序设计

2. 基于 VxWorks 的数据采集存储装置设计
3. Flash 文件系统分析及其在 VxWorks 中的实现
4. VxWorks 多任务编程中的异常研究
5. VxWorks 应用技巧两例
6. 一种基于 VxWorks 的飞行仿真实时管理系统
7. 在 VxWorks 系统中使用 TrueType 字库
8. 基于 FreeType 的 VxWorks 中文显示方案
9. 基于 Tilcon 的 VxWorks 简单动画开发
10. 基于 Tilcon 的某武器显控系统界面设计
11. 基于 Tilcon 的综合导航信息处理装置界面设计
12. VxWorks 的内存配置和管理
13. 基于 VxWorks 系统的 PCI 配置与应用
14. 基于 MPC8270 的 VxWorks BSP 的移植
15. Bootrom 功能改进经验谈
16. 基于 VxWorks 嵌入式系统的中文平台研究与实现
17. VxBus 的 A429 接口驱动
18. 基于 VxBus 和 MPC8569E 千兆网驱动开发和实现
19. 一种基于 vxBus 的 PPC 与 FPGA 高速互联的驱动设计方法
20. 基于 VxBus 的设备驱动开发
21. 基于 VxBus 的驱动程序架构分析
22. 基于 VxBus 的高速数据采集卡驱动程序开发
23. Vxworks 下的冗余 CAN 通讯模块设计
24. WindML 工业平台下开发 S1d13506 驱动及显示功能的实现
25. WindML 中 Mesa 的应用
26. VxWorks 下图形用户界面开发中双缓冲技术应用
27. VxWorks 上的一种 GUI 系统的设计与实现
28. VxWorks 环境下 socket 的实现
29. VxWorks 的 WindML 图形界面程序的框架分析
30. VxWorks 实时操作系统及其在 PC104 下以太网编程的应用
31. 实时操作系统任务调度策略的研究与设计
32. 军事指挥系统中 VxWorks 下汉字显示技术
33. 基于 VxWorks 实时控制系统中文交互界面开发平台
34. 基于 VxWorks 操作系统的 WindML 图形操控界面实现方法
35. 基于 GPU FPGA 芯片原型的 VxWorks 下驱动软件开发
36. VxWorks 下的多串口卡设计
37. VxWorks 内存管理机制的研究
38. T9 输入法在 Tilcon 下的实现
39. 基于 VxWorks 的 WindML 图形界面开发方法
40. 基于 Tilcon 的 IO 控制板可视化测试软件的设计和实现
41. 基于 VxWorks 的通信服务器实时多任务软件设计
42. 基于 VXWORKS 的 RS485MVB 网关的设计与实现
43. 实时操作系统 VxWorks 在微机保护中的应用

44. 基于 VxWorks 的多任务程序设计及通信管理
45. 基于 Tilcon 的 VxWorks 图形界面开发技术
46. 嵌入式图形系统 Tilcon 及应用研究
47. 基于 VxWorks 的数据采集与重演软件的图形界面的设计与实现
48. 基于嵌入式的 Tilcon 用户图形界面设计与开发
49. 基于 Tilcon 的交互式多页面的设计
50. 基于 Tilcon 的嵌入式系统人机界面开发技术
51. 基于 Tilcon 的指控系统多任务人机交互软件设计
52. 基于 Tilcon 航海标绘台界面设计
53. 基于 Tornado 和 Tilcon 的嵌入式 GIS 图形编辑软件的开发

Linux：

1. Linux 程序设计第三版及源代码
2. NAND FLASH 文件系统的设计与实现
3. 多通道串行通信设备的 Linux 驱动程序实现
4. Zsh 开发指南-数组
5. 常用 GDB 命令中文速览
6. 嵌入式 C 进阶之道
7. Linux 串口编程实例
8. 基于 Yocto Project 的嵌入式应用设计
9. Android 应用的反编译
10. 基于 Android 行为的加密应用系统研究
11. 嵌入式 Linux 系统移植步步通
12. 嵌入式 CC++语言精华文章集锦
13. 基于 Linux 的高性能服务器端的设计与研究
14. S3C6410 移植 Android 内核
15. Android 开发指南中文版
16. 图解 Linux 操作系统架构设计与实现原理（第二版）
17. 如何在 Ubuntu 和 Linux Mint 下轻松升级 Linux 内核
18. Android 简单 mp3 播放器源码
19. 嵌入式 Linux 系统实时性的研究
20. Android 嵌入式系统架构及内核浅析
21. 基于嵌入式 Linux 操作系统内核实时性的改进方法研究
22. Linux TCP IP 协议详解
23. Linux 桌面环境下内存去重技术的研究与实现
24. 掌握 Android 7.0 新增特性 Quick Settings
25. Android 应用逆向分析方法研究
26. Android 操作系统的课程教学

27. Android 智能手机操作系统的研究
28. Android 英文朗读功能的实现
29. 基于 Yocto 订制嵌入式 Linux 发行版
30. 基于嵌入式 Linux 的网络设备驱动设计与实现
31. 如何高效学习嵌入式
32. 基于 Android 平台的 GPS 定位系统的设计与实现
33. LINUX ARM 下的 USB 驱动开发
34. Linux 下基于 I2C 协议的 RTC 驱动开发
35. 嵌入式下 Linux 系统设备驱动程序的开发
36. 基于嵌入式 Linux 的 SD 卡驱动程序的设计与实现
37. Linux 系统中进程调度策略
38. 嵌入式 Linux 实时性方法
39. 基于实时 Linux 计算机联锁系统实时性分析与改进
40. 基于嵌入式 Linux 下的 USB30 驱动程序开发方法研究
41. Android 手机应用开发之音乐资源播放器
42. Linux 下以太网的 IPv6 隧道技术的实现
43. Research and design of mobile learning platform based on Android
44. 基于 linux 和 Qt 的串口通信调试器调的设计及应用
45. 在 Linux 平台上基于 QT 的动态图像采集系统的设计
46. 基于 Android 平台的医护查房系统的研究与设计
47. 基于 Android 平台的软件自动化监控工具的设计开发
48. 基于 Android 的视频软硬解码及渲染的对比研究与实现
49. 基于 Android 移动设备的加速度传感器技术研究
50. 基于 Android 系统振动测试仪研究
51. 基于缓存竞争优化的 Linux 进程调度策略

Windows CE:

1. Windows CE.NET 下 YAFFS 文件系统 NAND Flash 驱动程序设计
2. Windows CE 的 CAN 总线驱动程序设计
3. 基于 Windows CE.NET 的 ADC 驱动程序实现与应用的研究
4. 基于 Windows CE.NET 平台的串行通信实现
5. 基于 Windows CE.NET 下的 GPRS 模块的研究与开发
6. win2k 下 NTFS 分区用 ntldr 加载进 dos 源代码
7. Windows 下的 USB 设备驱动程序开发
8. WinCE 的大容量程控数据传输解决方案设计
9. WinCE6.0 安装开发详解
10. DOS 下仿 Windows 的自带计算器程序 C 源码
11. G726 局域网语音通话程序和源代码

12. WinCE 主板加载第三方驱动程序的方法
13. WinCE 下的注册表编辑程序和源代码
14. WinCE 串口通信源代码
15. WINCE 的 SD 卡程序[可实现读写的源码]
16. 基于 WinCE 的 BootLoader 研究
17. Windows CE 环境下无线网卡的自动安装
18. 基于 Windows CE 的可视电话的研究与实现
19. 基于 WinCE 的嵌入式图像采集系统设计
20. 基于 ARM 与 WinCE 的掌纹鉴别系统
21. DCOM 协议在网络冗余环境下的应用
22. Windows XP Embedded 在变电站通信管理机中的应用
23. XPE 在多功能显控台上的开发与应用
24. 基于 Windows XP Embedded 的 LKJ2000 仿真系统设计与实现
25. 虚拟仪器的 Windows XP Embedded 操作系统开发
26. 基于 EVC 的嵌入式导航电子地图设计
27. 基于 XPEmbedded 的警务区 SMS 指挥平台的设计与实现
28. 基于 XPE 的数字残币兑换工具开发

PowerPC：

1. Freescale MPC8536 开发板原理图
2. 基于 MPC8548E 的固件设计
3. 基于 MPC8548E 的嵌入式数据处理系统设计
4. 基于 PowerPC 嵌入式网络通信平台的实现
5. PowerPC 在车辆显控系统中的应用
6. 基于 PowerPC 的单板计算机的设计
7. 用 PowerPC860 实现 FPGA 配置
8. 基于 MPC8247 嵌入式电力交换系统的设计与实现
9. 基于设备树的 MPC8247 嵌入式 Linux 系统开发
10. 基于 MPC8313E 嵌入式系统 UBoot 的移植
11. 基于 PowerPC 处理器 SMP 系统的 UBoot 移植
12. 基于 PowerPC 双核处理器嵌入式系统 UBoot 移植
13. 基于 PowerPC 的雷达通用处理机设计
14. PowerPC 平台引导加载程序的移植
15. 基于 PowerPC 嵌入式内核的多串口通信扩展设计
16. 基于 PowerPC 的多网口系统抗干扰设计
17. 基于 MPC860T 与 VxWorks 的图形界面设计
18. 基于 MPC8260 处理器的 PPMC 系统

19. 基于 PowerPC 的控制器研究与设计
20. 基于 PowerPC 的模拟量输入接口扩展
21. 基于 PowerPC 的车载通信系统设计
22. 基于 PowerPC 的嵌入式系统中通用 IO 口的扩展方法
23. 基于 PowerPC440GP 型微控制器的嵌入式系统设计与研究
24. 基于双 PowerPC 7447A 处理器的嵌入式系统硬件设计
25. 基于 PowerPC603e 通用处理模块的设计与实现
26. 嵌入式微机 MPC555 驻留片内监控器的开发与实现
27. 基于 PowerPC 和 DSP 的电能质量在线监测装置的研制
28. 基于 PowerPC 架构多核处理器嵌入式系统硬件设计
29. 基于 PowerPC 的多屏系统设计
30. 基于 PowerPC 的嵌入式 SMP 系统设计

ARM：

1. 基于 DiskOnChip 2000 的驱动程序设计及应用
2. 基于 ARM 体系的 PC-104 总线设计
3. 基于 ARM 的嵌入式系统中断处理机制研究
4. 设计 ARM 的中断处理
5. 基于 ARM 的数据采集系统并行总线的驱动设计
6. S3C2410 下的 TFT LCD 驱动源码
7. STM32 SD 卡移植 FATFS 文件系统源码
8. STM32 ADC 多通道源码
9. ARM Linux 在 EP7312 上的移植
10. ARM 经典 300 问
11. 基于 S5PV210 的频谱监测设备嵌入式系统设计与实现
12. Uboot 中 start.S 源码的指令级的详尽解析
13. 基于 ARM9 的嵌入式 Zigbee 网关设计与实现
14. 基于 S3C6410 处理器的嵌入式 Linux 系统移植
15. CortexA8 平台的μC-OSⅡ及 LwIP 协议栈的移植与实现
16. 基于 ARM 的嵌入式 Linux 无线网卡设备驱动设计
17. ARM S3C2440 Linux ADC 驱动
18. ARM S3C2440 Linux 触摸屏驱动
19. Linux 和 Cortex-A8 的视频处理及数字微波传输系统设计
20. Nand Flash 启动模式下的 Uboot 移植
21. 基于 ARM 处理器的 UART 设计
22. ARM CortexM3 处理器故障的分析与处理
23. ARM 微处理器启动和调试浅析

24. 基于 ARM 系统下映像文件的执行与中断运行机制的实现
25. 中断调用方式的 ARM 二次开发接口设计
26. ARM11 嵌入式系统 Linux 下 LCD 的驱动设计
27. Uboot 在 S3C2440 上的移植
28. 基于 ARM11 的嵌入式无线视频终端的设计
29. 基于 S3C6410 的 Uboot 分析与移植
30. 基于 ARM 嵌入式系统的高保真无损音乐播放器设计
31. UBoot 在 Mini6410 上的移植
32. 基于 ARM11 的嵌入式 Linux NAND FLASH 模拟 U 盘挂载分析与实现
33. 基于 ARM11 的电源完整性分析
34. 基于 ARM S3C6410 的 uboot 分析与移植
35. 基于 S5PC100 移动视频监控终端的设计与实现

Hardware：

1. DSP 电源的典型设计
2. 高频脉冲电源设计
3. 电源的综合保护设计
4. 任意波形电源的设计
5. 高速 PCB 信号完整性分析及应用
6. DM642 高速图像采集系统的电磁干扰设计
7. 使用 COMExpress Nano 工控板实现 IP 调度设备
8. 基于 COM Express 架构的数据记录仪的设计与实现
9. 基于 COM Express 的信号系统逻辑运算单元设计
10. 基于 COM Express 的回波预处理模块设计
11. 基于 X86 平台的简单多任务内核的分析与实现
12. 基于 UEFI Shell 的 PreOS Application 的开发与研究
13. 基于 UEFI 固件的恶意代码防范技术研究
14. MIPS 架构计算机平台的支持固件研究
15. 基于 UEFI 固件的攻击验证技术研究
16. 基于 UEFI 的 Application 和 Driver 的分析与开发
17. 基于 UEFI 的可信 BIOS 研究与实现
18. 基于 UEFI 的国产计算机平台 BIOS 研究
19. 基于 UEFI 的安全模块设计分析
20. 基于 FPGA NiosⅡ的等精度频率计设计
21. 基于 FPGA 的 SOPC 设计
22. 基于 SOPC 基本信号产生器的设计与实现
23. 基于龙芯平台的 PMON 研究与开发
24. 基于 X86 平台的嵌入式 BIOS 可配置设计

25. 基于龙芯 2F 架构的 PMON 分析与优化
26. CPU 与 GPU 之间接口电路的设计与实现
27. 基于龙芯 1A 平台的 PMON 源码编译和启动分析
28. 基于 PC104 工控机的嵌入式直流监控装置的设计
29. GPGPU 技术研究与发展
30. GPU 实现的高速 FIR 数字滤波算法
31. 一种基于 CPUGPU 异构计算的混合编程模型
32. 面向 OpenCL 模型的 GPU 性能优化
33. 基于 GPU 的 FDTD 算法
34. 基于 GPU 的瑕疵检测
35. 基于 GPU 通用计算的分析与研究
36. 面向 OpenCL 架构的 GPGPU 量化性能模型
37. 基于 OpenCL 的图像积分图算法优化研究
38. 基于 OpenCL 的均值平移算法在多个众核平台的性能优化研究
39. 基于 OpenCL 的异构系统并行编程
40. 嵌入式系统中热备份双机切换技术研究

Programming:

1. 计算机软件基础数据结构 - 算法
2. 高级数据结构对算法的优化
3. 零基础学算法
4. Linux 环境下基于 TCP 的 Socket 编程浅析
5. Linux 环境下基于 UDP 的 socket 编程浅析
6. 基于 Socket 的网络编程技术及其实现
7. 数据结构考题 - 第 1 章 绪论
8. 数据结构考题 - 第 2 章 线性表
9. 数据结构考题 - 第 2 章 线性表 - 答案
10. 基于小波变换与偏微分方程的图像分解及边缘检测
11. 基于图像能量的布匹瑕疵检测方法
12. 基于 OpenCL 的拉普拉斯图像增强算法优化研究
13. 异构平台上基于 OpenCL 的 FFT 实现与优化

FPGA / CPLD:

1. 一种基于并行处理器的快速车道线检测系统及 FPGA 实现

2.