基于 FPGA 的 AES 加密算法的高速实现

High speed implementation of AES algorithm based on FPGA

(中南大学) 马 肃 王 击
MA Su WANG Ji

摘要: 介绍 AES 算法的原理以及基于 FPGA 的高速实现。结合算法和 FPGA 的特点,采用查表法优化处理了字节代换运算、列混合运算。同时,为了提高系统工作速度,在设计中应用了内外结合的流水线技术,并应用 Altera 公司的开发工具及芯片进行实际开发。

关键词: AES; FPGA; 查表法; 流水线技术
中图分类号: TP271+.5　　**文献标识码:** B

Abstract: This paper describes the design of AES and fast implementations of AES on hardware based on FPGA.Based on the characteristic of AES and FPGA,the implementation of subbytes, mixcolumns is optimized by using the method of look-up tables.For making it work faster,the pipelining method is taken in the design.The develop tools and IC are from the Altera company.

Key words: AES; FPGA; method of look-up tables; Pipeline Technology

1 引言

随着信息技术的迅速发展, 信息已成为当今社会的一种重要资源。但当人们享受信息资源带来的巨大便利的同时,也承受着信息被篡改、泄漏、伪造的威胁,安全问题日益严重。安全风险制约着信息的有效使用,信息安全对现代社会健康有序的发展,保障国家安全和社会稳定有着重要作用。加密技术是信息安全技术的核心,是保证信息资源安全的关键。

高级加密标准(Advanced Encryption Standard, AES)作为传统对称加密算法标准 DES 的替代者,由美国国家标准与技术研究所(NIST)于 1997 年提出征集该算法的公告,2000 年最终选定了 Rijndael 算法, 并于 2001 年正式发布了 AES 标准。Rijndael 算法本质上是一种对称分组密码体制,该算法汇聚了安全性能、效率、可实现性和灵活性等优点,已经成为工业界、银行业、政府部门的事实上的密码标准。

随着网络传输速度的快速提升, 业界对算法的执行速度的要求也越来越高,基于软件的密码算法便显得性能不足,需要采用硬件加密的方式。另外,用硬件实现加密算法具有较更高的物理安全性。而 FPGA 芯片兼有硬件的安全性和高速性以及软件的灵活性和易维护性,从而成为研究和实现 AES 算法的理想硬件平台。

2 AES 加密算法简介

AES 是一种分组迭代密码, 明文分组长度固定为 128 b,而且仅支持 128,196 或 256 b 的密钥长度,本文着重对密钥长度为 128 b 的情况进行讨论。AES 加密算法的实现流程如图 1 所示,将输入的明文填入一个 4X4 的矩阵(16 进制),并将其称为状态矩阵。算法的前 round-1 轮包含四种变换,分别是:字节替换、轮密钥加、行移位、列混合。对于每一轮,都有对应的子密钥。子密钥由初始密钥通过密钥扩展得到。最后一轮由字节替换、行移位和轮密钥加组成。AES 解密过程为上述过程的逆过程。

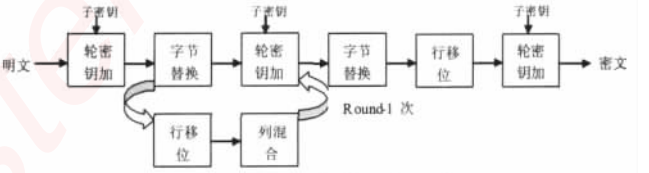

图 1 AES 加密算法实现流程

字节替换:字节替换(SubBytes)是一个基于 S 盒的非线性置换, 它通过一个简单的查表操作将输入或中间状态的每一个字节映射为另一个字节。 查表的方法为:将输入字节的高 4 位作为 S 盒的行值,低 4 位作为列值,然后取出 S 盒中对应行和列的元素作为输出。

行移位:行移位(ShiftRows)完成基于行的循环移位操作。具体的操作为:第 0 行不动,第 1 行循环左移 1 个字节,第 2 行循环左移 2 个字节,第 3 行循环左移 3 个字节。

列混合:列混合(MixColumns)是对状态矩阵中的列做线性变换,进行四字节乘运算。具体定义如下:将状态矩阵的列看作有限域 $G(2^8)$上的多项式,并在模 x^4+1 下与一个给定的多项式 c(x) 相乘,其中 $c(x)=03x^3+01x^2+01x+02$。假设该步变换状态的一列输入为 a,输出为 b,即 $b(x)=c(x)\cdot a(x) \bmod (x^4+1)$。

密钥加:密钥加(AddRoundKey)是将轮密钥的各字节和状态矩阵中相应位置的字节分别模 2 加,实现状态和密钥的混合。轮密钥的长度和状态的长度是一样的。该步骤的逆变换是其自身

3 算法实现的优化

3.1 对算法本身的优化

用查找表和组合逻辑的方式代替了复杂的乘法运算, 大大减少了芯片资源的占用,提高了加、解密步骤的执行速度。

字节替换是 Rijndael 密码中唯一的非线性变换。该步骤是一种非线性面向字节的变换, 是将一个 8 位二进制数据转换为另一个不同的 8 位二进制数据,这里要求一一对应,并且替换结

案中能超出 8 位,可以通过构造可逆的 S-盒来实现。由于有限域 GF(2)中总共有 256 个元素,则可预先通过一定的算法计算出每个元素的逆元,再进行对应的仿射变换求出有限域 $GF(2^8)$中每个元素经过字节代换后所对应的值,并将这个计算出的替代值写入一个 16×16 字节的置换表中相应的位置作为步骤 SubBytes 的 S-盒。具体实现时,根据状态的每一个字节的数值检索出 S-盒中对应的替代值,即通过查表即可实现该步变换,避免复杂的乘法运算。

对于列混合变换,由于 $GF(2^8)$有限域中的每一个元素都能够写成 02 的不同幂次的和,因此,乘以任何常数的乘法都可以通过反复的乘以 02 和异或运算来实现。可将矩阵乘法中的常数因子分解为 02 的不同幂次和,矩阵乘法转换为与 02 的乘法和异或运算。将 $GF(2^8)$域中的每一个元素与 02 的乘积存储在一张 16×16 字节查找表中,记作 xtime(·)。所以,该步骤可以通过查表和异或运算实现。

3.2 加密模块结构的优化

加密模块结构直接影响 AES 算法的加解密速度,AES 算法加解密系统的速度是指单位时间内完成的加密(解密)的比特数,也称为吞吐量(throughput),单位为兆比特每秒(Mbit/s)。其基本结构可分为以下三种:外部流水线结构、内部流水线结构和循环展开结构。其中循环展开结构的速度是以芯片面积增加为代价的,而外部流水线结构和内部流水线结构在反馈模式中速度受到限制,面积的增加并不能增加速度,所以这两种结构只适用于非反馈模式。内部流水线结构的速度在非反馈模式下随着内部流水线站数的增加而增加,但面积的相应增长极小,具有很好的速度面积比。但在反馈模式下其速度面积比不具优势。因此,在外部应用流水线结构设计的同时,在内部划分流水线站,可以在外部流水线结构的速度基础上进一步提高速度,而面积的增长极小,从而提高吞吐量和速度面积比。基于以上分析,在本设计中采取了非反馈模式和内外混合的流水线结构。

4 硬件测试及应用

本设计采用 ALTERA 公司的开发工具 QuartusII,以 VerilogHDL 为实现语言,在综合仿真并测试无误后,下载至 ALTERA 公司的 Cyclone 系列芯片上。该系列芯片具有相当的性价比,非常适合于大批量、低成本的应用本设计方案。本设计既可以作为单独的专用加密芯片完成加密任务,也可以嵌入到复杂的数字系统中。具有非常广阔的应用市场。

本文作者创新点:对 AES 算法的实现进行研究,根据硬件实现的特点,使用查表的方法以及内外流水线相结合的结构实现。

参考文献

[1]胡向东,魏琴芳.应用密码学教程.北京:电子工业出版社[M],73-76.

[2]E Rodriguez-Henriquez, N.A. Saqib and A. Diaz-Pkrez. 4.2 Gbit/s single-chip FPGA implementation of AES algorithm.ELECTRONICS LETTERS[M].

[3]李艳俊,李彦兵,毛明,欧海文.简化 AES 的设计和可视化实现[J].微计算机信息,2008,4-3:72-73.

[4]Swinder Kaur, Renu Vig. Efficient Implementation of AES Algorithm in FPGA Device. International Conference on Computational Intelligence and Multimedia Applications 2007[J].

[5]Marko Mali,Franc Novak,Anton Biasizzo.Hardware impletation of AES algorithm[M].

作者简介:马肃(1982-),男,中南大学硕士研究生,现主要从事 EDA 技术及应用的研究;王击(1968-),男,中南大学副教授,主要研究领域:嵌入式系统、楼宇自动化、电力系统及其自动化、智能控制。

Biography: MA Su (1982-),Male,Hunan,CenterSouth University, Master,Research area:the application and research of EDA.

(410083 湖南长沙 中南大学) 马 肃 王 击

通讯地址:(410083 湖南长沙 中南大学本部民主楼 113) 马 肃

(收稿日期:2008.11.10)(修稿日期:2009.02.10)

(上接第 112 页)

安全与数据加密问题。本文设计实现的动态口令终端系统将在各网络平台中应用推广,届时将会在越来越多的商业场合得到广泛应用。预计 5 年内整个项目手机用户使用的带动态口令功能的 ARM7 智能卡片可达 100 多万片,产生经济效益可达 1500 多万元。

本文作者创新点是利用手机终端 STK 功能扩展技术,采用 ARM7 智能卡硬件平台为动态口令终端提供一种全新的方案,该方案在不影响原有手机及 SIM 卡功能的基础上,借助手机屏幕实现动态口令显示,既保证了动态口令的安全性,又解决了以往口令终端存在的不足。

参考文献

[1]顾韵华,刘素英. 动态口令身份认证机制及其安全性研究[J]. 微计算机信息. 2007,11 -3:51-53。

[2]张明杰,罗毅, 牛汉春. 基于 SIM 卡动态口令的互联网身份认证体系与应用[J]. 电信科学. 2007 年第 12 期

[3]宾志滔. 手机通用功能扩展器. 中国专利. 200620035611.0 .

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
70. CAN 总线的浅析 CANopen 协议
71. 基于 CANopen 协议实现多电机系统实时控制
72. 以太网时钟同步协议的研究

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. 基于 FPGA 和 DSP 的 DBF 实现
3. 高速浮点运算单元的 FPGA 实现
4. DLMS 算法的脉动阵结构设计及 FPGA 实现
5. 一种基于 FPGA 的 3DES 加密算法实现
6.