基于 TLS 协议的 ECC 扩展研究

张建林，寇　兰

(重庆邮电大学通信与信息工程学院，重庆 400065)

摘　要：根据 TLS 握手协议的工作流程，分析椭圆曲线密码体制 ECC 对 TLS 协议所做的算法扩展。设计实现 ECDSA 数字签名和 ECDH 密钥交换算法的扩展，并对基于 TLS 握手协议的X.509 证书作 ECDSA 算法扩展研究。

关键词：TLS；ECC；ECDSA；ECDH；X.509 证书

Research on ECC extension based on TLS protocol

ZHANG Jian-lin，KOU Lan

(**School of Communication and Information Engineering，Chongqing University of Posts and Telecommunications，Chongqing** 400065，**China**)

Abstract：This paper introduced the extension of ECC based on the mechanism of TLS handshake protocol. The digital signature algorithm based on Elliptic Curve Cryptosystem (ECDSA) and Diffie-Hellman algorithm based on Elliptic Curve Cryptosystem (ECDH) were presented. The X.509 certificate based on TLS handshake protocol is also extended to support ECC digital signature.

Key words：TLS；ECC；ECDSA；ECDH；X.509 certificate

0　引言

随着计算机技术的发展及互联网的普及应用，电子商务业务蓬勃发展。为保护数据信息安全，建立了安全的电子商务环境，人们便采用各种密码安全协议。安全套接层 SSL (Secure Socket Layer) 协议正是一种基于公私钥加解密体制 (PKI) 的网络数据安全协议，它基于 TCP/IP 的客户/服务器应用程序提供客户端和服务器的认证、数据完整性及机密性等安全措施。SSL 协议被广泛地应用于 Internet 上，后被发展为 TLS (Transport Layer Security) 协议，成为网络安全工业标准的一部分。

在大多数安全应用中，TLS 协议利用 RSA 公钥密码体制在通信实体间交换传递加密密钥。随着大整数分解方法的研究及计算机速度的提高，RSA 所需的密钥愈来愈长，使得采用 RSA 加密体制的系统效率愈来愈低，为此需要寻求一种高效的公钥密码算法。而椭圆曲线密码算法 ECC 能以更小的密钥尺寸提供与其他公钥密码算法相同的安全等级，即 ECC 能提供比 RSA 更高的安全性，同时能有效提高 TLS 协议的性能，有选择 ECC 代替 RSA 的必要。

本文通过对 TLS 协议进行椭圆曲线密码算法扩展，使扩展后的协议能利用椭圆曲线密码体制在通信实体间交换随机密钥，提高 TLS 协议的安全性和效率性，以满足实际应用的需求。

1　TLS 协议分析

TLS 协议是建立通信实体间端到端安全会话的通道，提供机密性和数据完整性。该协议是独立于应用协议的，高层协议可以透明地分布在 TLS 协议之上。协议由 TLS 记录协议 (TLS record protocol) 和 TLS 握手协议 (TLS handshake protocol) 两层组成。TLS 记录协议处于 TLS 协议的底层，位于某一可靠的通信协议 (如 TCP 协议) 之上，用于透明封装各高级应用层协议，在客户机和服务器之间传输高层应用数据和 TLS 控制数据，并有可能对数据进行分段或组合。TLS 握手协议位于 TLS 协议的高层，用于

服务器与客户机在应用程序协议传输和接收其第一个数据字节前彼此相互认证,协商加密算法和加密密钥[1]。本文仅讨论与 TLS 握手协议有关的内容。

TLS 握手协议用于实际的数据传输开始之前,提供客户和服务器相互认证,协商加密和 MAC 算法以及保密密钥,保护 TLS 记录协议发送的数据。TLS 的传输过程需要先进行握手,用公钥密码算法使服务器端在客户端得到验证,验证完成后就可以使用双方协商成功的密钥加密、解密数据。TLS 握手协议用于完成以下 4 种功能:(1)协商客户与服务器之间数据传送使用的密码组;(2)建立和共享客户与服务器之间的会话密钥;(3)客户认证服务器(可选);(4)服务器认证客户(可选)。TLS 握手协议的过程会根据配置服务器证书的要求或客户端证书的请求而有所不同。

2 椭圆曲线密码体制

椭圆曲线密码体制(Elliptic Curve Cryptosystem)ECC 自 1985 年问世以来,受到全世界密码学家、数学家和计算机科学家的广泛关注。ECC 属于公钥加密算法,其安全性是基于椭圆曲线点群上离散对数问题(ECDLP)的难解性[2]。ECDLP 是比整数因子分解问题 IFP 和离散对数问题 DLP 难得多的数学难题,这意味着 ECC 能以更小的密钥尺寸产生与其他公钥密码算法相同等级的安全性。

ECC 的技术优势主要表现在安全性能高、计算量小、处理速度快、存储空间小、带宽要求低,使得应用该算法的系统参数小、公钥小、节省带宽、执行速度快、硬件要求低。

ECC 的这些优点使它必将取代 RSA,成为通用的公钥密码算法。因此,在 TLS 协议中扩展椭圆曲线密码算法显得尤为必要。RSA 与 ECC 安全性比较如表 1 所示。

表 1 RSA 与 ECC 安全性比较

ECC 密钥尺寸(bits)	RSA 密钥尺寸(bits)	密钥尺寸比率	AES 密钥尺寸(bits)
163	1024	1∶6	
256	3072	1∶12	128
384	7680	1∶20	192
512	15360	1∶30	256

3 TLS 协议的 ECC 扩展

基于对 TLS 协议中握手协议工作过程的分析,对 TLS 协议作以下 ECC 扩展。

(1)扩展基于 ECC 的密钥交换算法。

(2)扩展 ECC 证书。

(3)扩展椭圆曲线及曲线上点格式。

3.1 扩展基于 ECC 的密钥交换算法

参照 DH_DSS, DHE_DSS, DH_RSA, DHE_RSA 以及 DH_anon,对基于 ECC 的 ECDH 算法和 ECDSA 算法进行扩展,如图 2 所示。

表 2 基于 ECC 的密钥交换算法

密钥交换算法		算法相关说明
ECDH	ECDSA	使用 ECDSA 签名的证书中的密钥对
ECDHE	ECDSA	临时生成 ECDH 密钥对的 ECDH,使用 ECDSA 算法签名
ECDH	RSA	使用 RSA 签名的证书中的密钥对
ECDHE	RSA	临时生成 ECDH 密钥对的 ECDH,使用 RSA 算法签名
ECDH	anon	匿名的 ECDH,无签名信息

基于 ECC 的密钥交换算法主要包含密钥交换和数字签名算法,实现的 ECC 扩展中包括 ECC 密码组的 ECDH 算法和 ECDSA 算法[3]。基于 ECC 的密钥交换算法均使用 ECDH 计算 TLS 初始共享密钥,区分在于 ECDH 密钥的生命周期(长期的或临时的)及认证机制(如果有)的不同。

ECDH_ECDSA 的服务器可获取 ECC 密钥和证书认证,适于不支持 RSA 的受限设备。ECDH_RSA 需要服务器获取 ECC 证书,但证书的发行者仍可使用 RSA 密钥签名,可消除更新 TLS 客户可信证书认证密钥的必要性。

ECDHE_ECDSA 和 ECDHE_RSA 密钥交换机制提供前向安全性。ECDHE_RSA 服务器能利用 RSA 证书并遵从受限客户的椭圆曲线的参数选择。然而,ECDHE_RSA 服务器的计算量是远大于不提供前向安全性的 RSA 密钥交换。

ECDH_anon 密钥交换算法不提供服务器或客户的认证。与其他匿名 TLS 密钥交换算法一样,常受到中间人攻击。则基于此算法的设备应当提供其他方式的认证。

3.2 扩展支持 ECC 算法的 X.509 证书

X.509 证书是当前使用最广泛的一种证书格式。由以下 4 个部分组成:证书内容、主体公钥信息、证书签发者的签名信息及证书扩展项(可选)[4]。

证书内容由以下几部分组成:①X.509 v3 版本号。②CA 发放证书的序列号。③发行者 CA 的唯一标识名。④证书的生效和失效时间范围。⑤主体(证书所有者)唯一标识名。

主体公钥信息由三个部分组成:①主体公钥算法标识 ECC 公钥的对象标识。②算法参数:字符串类型,其编码方法由算法决定。③主体公钥:主体的公开密钥,由算法标识和公钥值组成。

证书签发者的签名信息由三个部分组成:①签名算法标识:CA 使用 SHA1 消息摘要算法和 ECDSA 签名算法对证书签名。②签名算法参数:签名算法参数从 CA 根证书的主体公钥信息中获得。③数字签名:计算证书的 SHAI 消息摘要和 ECDSA 数字签名,将签名值作为 BIT STRING 类型的 ASN1 编码保存于该字段中。

在 TLS 握手协议中,客户或服务器认证需要通过 CA 证书来完成,因此,扩展的 CA 证书需支持 ECC 算法的签名与认证。实现的 X.509 v3 证书的 ECC 扩展,可根据给定的 ECC 参数生成 X.509 格式的 ECDSA 签名证书,应用于 TLS 握手协议中[5]。

3.3 扩展椭圆曲线和曲线上点格式

在 TLS 握手开始新的连接阶段,新的 TLS 扩展允许使用特殊椭圆曲线和点格式(例如压缩,解压缩),以支持相应的受限客户。在客户 ClientHello 消息中,客户端列举所支持的曲线及点格式的扩展。同样,在服务器 ServerHello 消息中,服务器端也列举所支持的曲线及点格式的扩展。

TLS 客户端可选择 ECC 加密组在客户 ClientHello 消息中包含椭圆曲线和点格式的扩展。而 TLS 服务器在服务器 ServerHello 消息中必须支持这些扩展,可自由选择相应的曲线或点格式。当客户使用这些扩展时,服务器不必协商 ECC 加密组(除非客户特别说明选择相应的曲线和压缩技术)。因而,在协商 ECC 握手过程中,不存在客户不能处理服务器椭圆曲线密钥而中止的可能性。

在会话恢复阶段,服务器会忽略当前 ClientHello 消息中所支持的椭圆曲线扩展和点格式扩展。而这些扩展仅在握手协商新的阶段中起作用。

4 实现 TLS 协议的 ECC 扩展的安全性分析

基于 TLS 的 ECC 扩展并没有改变 TLS 协议的运行机制,也没有改变 TLS 握手协议的工作过程,因此,基于 ECC 扩展的 TLS 协议没有产生额外的安全机制问题。

通过 ECC 的扩展,TLS 协议可以选用较长的 ECC 密钥来进行密钥交换,也可选用更安全的 ECC 密钥尺寸的密钥来签名和认证,因此,附带 ECC 的扩展的 TLS 协议能提供更高级别的安全性。

5 结束语

通过实现 TLS 协议的 ECC 扩展,在 TLS 协议内部实现了 ECC 公钥密码算法,并对 TLS 协议使用的 X.509证书进行支持 ECC 算法的扩展,在满足当前应用的基础又增强了 TLS 协议的安全性。

参 考 文 献:

[1] The TLS Protocol[Z]. Version 1.1,RFC 4346, 2006.

[2] 冯飞,方琪,王令群. 基于椭圆曲线密码体制的系统设计[J]. 计算机时代,2005.

[3] Blake-Wilson S, Bolyard N, Gupta V,et al. Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)[C]. RFC4492, May 2006.

[4] 陆洁茹,朱艳琴. SSL 中 ECC 数字证书的设计与实现[J]. 计算机应用与软件,2007,24(12).

[5] 吕俊文,宋涛,司天歌,等. SSL 协议的 ECC 扩展实现[J]. 计算机工程与设计,2006,27(10):1715 - 1725.

责任编辑:么丽苹

(上接第 98 页)

启动前,主开关合闸,风力发电机组控制器准备自动运行。首先系统初始化,控制程序初始化、检查微控制器硬件和外设状态是否完好,检测系统参数(温度,液压油,压力,风向,风速等),比较所检测的操作参数,如果没有故障,系统就可以正式起动。启动时,首先检查电网,检测电网的各个参数、设置各个计数器、输出机构初始工作状态及晶闸管的开通角[3],之后,风力发电机组开始自动运行。风轮的叶尖角由 90°恢复为 0°,风轮开始转动,计算机开始实时监测各个参数,随着风轮速度的提高,风轮反馈的转速信号作为输入的判断条件,送入控制器,以判断是否可以并网。当发电系统运行以后,系统检测的参数用以判断参数有否超过极限、执行偏航、相位补偿、安全制动。

2 结束语

结合风力发电的控制要求,以 S7 - 300 型 PLC 模块为例,对 750kW 风力发电机组的控制系统进行了概述,研究了其控制系统的构成及风机控制过程,本文设计的 PLC 控制系统,通过测试风机的实际控制及运行可以实现对风电机组的良好控制。

参 考 文 献:

[1] 叶杭冶. 风力发电机组的控制技术[M]. 北京:机械工业出版社,2002:59 - 63.

[2] 叶启明. 大型风力发电机组系统的结构与特点[J]. 华中电力,2002:36 - 38.

[3] 张福田. 异步风力发电机并网运行的理论探讨[J]. 风力发电,1991(4):36 - 40.

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
73. 基于 CANopen 的列车通信网络实现研究
74. 基于 SJA1000 的 CAN 总线智能控制系统设计
75. 基于 CANopen 的运动控制单元的设计
76. 基于 STM32F107VC 的 IEEE 1588 精密时钟同步分析与实现

77. 分布式控制系统精确时钟同步技术
78. 基于 IEEE 1588 的时钟同步技术在分布式系统中应用
79. 基于 SJA1000 的 CAN 总线通讯模块的实现
80. 嵌入式设备的精确时钟同步技术的研究与实现
81. 基于 SJA1000 的 CAN 网桥设计
82. 基于 CAN 总线分布式温室监控系统的设计与实现
83. 基于 DSP 的 CANopen 通讯协议的实现
84. 基于 PCI9656 控制芯片的高速网卡 DMA 设计
85. 基于以太网及串口的数据采集模块设计
86. MVB1 类设备控制器的 FPGA 设计
87. MVB 接口彩色液晶显示诊断单元的显示应用软件设计
88. IPv6 新型套接字的网络编程剖析
89. 基于规则的 IPv4 源程序到 IPv6 源程序的移植方法
90. MVB 网络接口单元的 SOC 解决方案
91. 基于 IPSec 协议的 IPv6 安全研究
92. 具有 VME 总线的车载安全计算机 MVB 通信板卡
93. SD 卡的传输协议和读写程序
94. 基于 SCTP 的 TLS 应用
95. 基于 IPv6 的静态路由实验设计
96. 基于 MVB 的地铁列车司机显示系统研究
97. 基于参数优化批处理的 TLS 协议
98. SSD 数据结构与算法综述
99. 大容量 NAND Flash 文件系统中的地址映射算法研究
100. 基于 MVB 总线的动车组门控系统的设计与仿真研究

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

54. VxWorks 环境下内存文件系统的应用
55. VxWorks 下的多重定时器设计
56. Freescale 的 MPC8641D 的 VxWorks BSP
57. VxWorks 实验五[时间片轮转调度]
58. 解决 VmWare 下下载大型工程.out 出现 WTX Error 0x100de 的问题
59. 基于 VxWorks 系统的 MiniGUI 图形界面开发
60. VxWorks BSP 开发中的 PCI 配置方法
61. VxWorks 在 S3C2410 上的 BSP 设计
62. VxWorks 操作系统中 PCI 总线驱动程序的设计与实现
63. VxWorks 概述
64. 基于 AT91RM9200 的 VxWorks END 网络驱动开发
65. 基于 EBD9200 的 VxWorks BSP 设计和实现
66. 基于 VxWorks 的 BSP 技术分析
67. ARM LPC2210 的 VxWorks BSP 源码
68. 基于 LPC2210 的 VxWorks BSP 移植
69. 基于 VxWorks 平台的 SCTP 协议软件设计实现
70. VxWorks 快速启动的实现方法[上电到应用程序 1 秒]

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
52. Linux 基于 W83697 和 W83977 的 UART 串口驱动开发文档
53. 基于 AT91RM9200 的嵌入式 Linux 系统的移植与实现
54. 路由信息协议在 Linux 平台上的实现
55. Linux 下 IPv6 高级路由器的实现
56. 基于 Android 平台的嵌入式视频监控系统设计

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
29. Windows CENET 下 ADC 驱动开发设计
30. Windows CE 下 USB 设备流驱动开发与设计
31. Windows 驱动程序设计
32. 基于 Windows CE 的 GPS 应用
33. 基于 Windows CE 下大像素图像分块显示算法的研究
34. 基于 Windows CE 的数控软件开发与实现
35. NAND FLASH 在 WINCENET 系统中的应用设计

PowerPC：

WeChat ID: kontronn

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
31. 基于 MPC850 的多功能通信管理器
32. 基于 MPC8640D 处理系统的技术研究
33. 基于双核 MPC8641D 处理器的计算机模块设计
34. 基于 MPC8641D 处理器的对称多处理技术研究

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-OS II 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
36. UBoot 在 AT91RM9200 上的移植简析
37. 基于工控级 AT91RM9200 开发板的 UBoot 移植分析
38. 基于 ARM11 和 Zigbee 的人员定位防丢器
39. 基于 NAND FLASH 的嵌入式系统启动速度的研究

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
41. EFI-Tiano 环境下的 AES 算法应用模型
42. EFI 及其安全性研究
43. 基于 UEFI Shell 的 PreOS Application 的开发与研究
44. UEFI Bootkit 模型与分析
45. UEFI 计算机系统快速调试方法的实现

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
14. 数据结构考题 - 第 4 章 串
15. 数据结构考题 - 第 4 章 串答案
16. 用 IPv6 编程接口实现有连接通信的方法

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. 可编程 FIR 滤波器的 FPGA 实现
7. 基于 FPGA 的 AES 加密算法的高速实现

8. 基于 FPGA 的精确时钟同步方法
9. 应用分布式算法在 FPGA 平台实现 FIR 低通滤波器
10. 流水线技术在用 FPGA 实现高速 DSP 运算中的应用
11. 基于 FPGA 的 CAN 总线通信节点设计
12. 基于 FPGA 的高速时钟数据恢复电路的实现
13. 基于 FPGA 的高阶高速 FIR 滤波器设计与实现
14. 基于 FPGA 高效实现 FIR 滤波器的研究
15. FPGA 的 VHDL 设计策略
16. 用 FPGA 实现串口通信的设计
17. GPIB 接口的 FPGA 实现
18. 一种基于 FPGA 的 FFT 阵列处理器
19. 基于 FPGA 的 FFT 信号处理器的硬件实现