

基于 S3C4510B 的嵌入式实验室网关基本系统设计^{*})

张耀丹¹ 曾孝平 王红霞

(重庆大学通信工程学院 重庆 400030)

摘要 本文提出了一种基于 S3C4510B 和 uCLinux 操作系统的高性价比、可靠的嵌入式实验室网关的设计方案,目的是取代目前在实验室普遍使用的作为本地局域网网关的一台单独的计算机,以节约实验室资源、成本和空间。文中主要介绍了系统结构、系统硬件电路设计及系统 BootLoader 代码的设计与实现。

关键词 S3C4510B, 硬件电路, 实验室网关, BootLoader

Designing for Embedded Lab Gateway Based on S3C4510B

ZHANG Yao-Dan ZENG Xiao-Ping WANG Hong-Xia

(College of Communication Engineering, Chongqing University, Chongqing 400030)

Abstract Universally, there is an independent computer using as the local network's gateway in schools and labs, it waste the resource as a result. This paper provides a design scheme for embedded lab gateway based on S3C4510B and uCLinux OS. And introduce the system architecture, circuit design and BootLoader design.

Keywords S3C4510B, Hardware circuit, Lab gateway, BootLoader

在学校、实验室,普遍都是使用一台单独的计算机作为本地局域网网关,这样充当网关的计算机几乎不能另作它用,造成了资源的浪费,且充当网关的计算机必须占用一定的空间。而嵌入式网关具有性价比高、体积小等特点,且必要时才通过串口与计算机相连,进行配置、修改等操作,操作完后即可断开与计算机之间的连接,不影响计算机的正常使用,可有效节约资源。因此本文提出了一种低成本、高稳定性的嵌入式网关设计方案。系统结构如图 1 所示。嵌入式网关通过两个网口分别与实验室内部局域网集线器和外部网路由器相连。在需要时,可通过 PC 机的串口对嵌入式网关的各种参数进行配置。

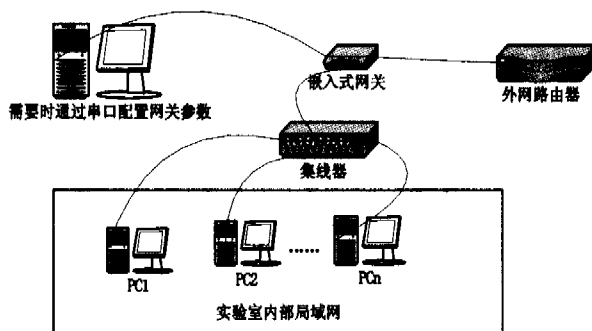


图 1 系统结构图

Samsung 公司的 S3C4510B 芯片是基于以太网应用系统

的高性价比 16/32 位 RISC 微处理器,内含一个由 ARM 公司设计的 16/32 位 ARM7TDMI RISC 处理器核,ARM7TDMI 为低功耗、高性能的 16/32 位核,最适合用于对价格及功耗敏感的应用场合。

本系统以 S3C4510B 为核心构建电路,其中双以太网口、串口设计是该系统的重点;系统在 S3C4510B 上移植 uCLinux 操作系统,文中详细介绍了其启动代码(BootLoader)的设计及实现。

1 系统硬件结构

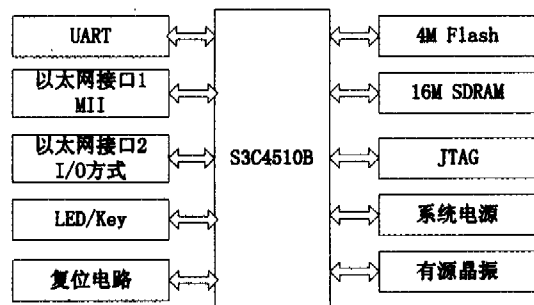


图 2 系统硬件结构图

图 2 所示为本系统硬件结构框图,系统以 S3C4510B 为核心,外围扩展一系列接口。

^{*}) 本项目为重庆大学研究生创新实践基地基金资助项目。张耀丹 硕士研究生,研究方向为嵌入式系统;曾孝平 博士(后),教授,博导,研究方向为信号处理技术;王红霞 硕士研究生,研究方向为软件无线电技术。

参考文献

- 1 ITU-T Recommendation H. 323 Draft v5. Packet-Based Multimedia Communications Systems [S]. 2003,5
- 2 Rosenberg J, Schulzrinne H. SIP: session Initiation Protocol. RFC 3261 [S]. 2000,6
- 3 ITU-T Recommendation H. 225.0. Call Signalling Protocols and Media Stream Packetization for Packet-based Multimedia Communication Systems [S]. 2000,2

- 4 ITU-T Recommendation H. 245 control protocol for multimedia communication [S]. 2003,5
- 5 舒华英,李勇,等. VOIP 技术与应用 [M]. 北京:人民邮电出版社,2003. 77~82
- 6 唐哲,黄本雄. H. 323 网络和 SIP 网络互通的寻址定位研究 [J]. 计算机工程,2004, 30(13): 29~31
- 7 IETF. draft-agrawal-sip-h323-interworking-reqs-06. txt [Z]. 2004,2
- 8 李劲峰,王文东,程时端. H. 323 与 SIP 互通的研究 [J]. 北京邮电大学学报,2000, 23(4): 50~53

Flash 采用的是两片 MBM29LV160 并联的方式构建 32 位存储系统,大小为 4MB,用于存放已调试好的启动代码(BootLoader)、用户应用程序、uCLinux 操作系统及其他在系统掉电以后需要保护的用户数据;SDRAM 采用的是两片 HY57V641620 并联的方式构建 32 位存储系统,大小为 16MB,其作为系统运行时的主要区域,操作系统及用户数据均位于 SDRAM 中。

系统电源电路为系统提供 5V、3.3V 两组电压,为 S3C4510B 及外围电路供电;10MHz 的有源晶振为系统提供工作时钟,通过片内 PLL 电路倍频为 50MHz 作为微处理器的工作时钟;JTAG 接口可对芯片内部的所有部件进行访问,通过该接口可对系统进行软硬件调试、编程等;复位电路采用 74HC04,可完成系统上电复位和在系统工作时的用户按键复位。

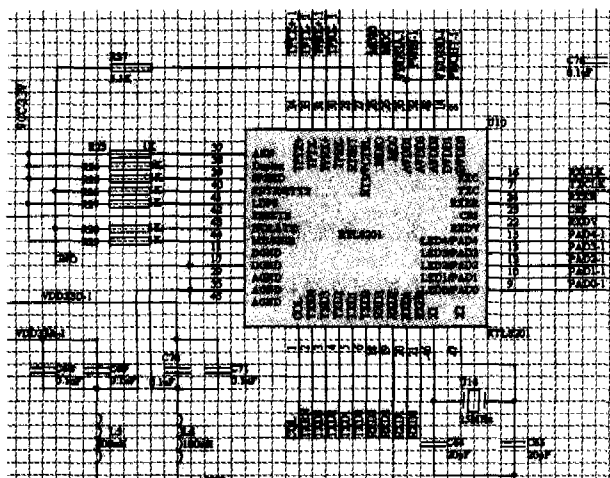
UART 电路采用 MAX232 芯片,用于 S3C4510B 系统与 PC 机的短距离双向串行通信,在本系统中用户可通过串口配置网关的 IP 地址、MAC 地址等主要参数。

以太网接口部分为本嵌入式网关系统的核心及创新部分,其中接口 1 采用媒体独立接口(MII)方式,选用 RTL8201 芯片,接口 2 采用 I/O 方式,选用 RTL8019AS 芯片,此两个接口为系统提供以太网接入的物理通道,通过该接口,系统可以以 10Mbps/100Mbps 的速率接入以太网,接口 1 和接口 2 在本系统中分别用作与实验室局域网内网和外网的接口。

下面将详细介绍双以太网口和 UART 接口的设计方案。

2 双以太网接口硬件设计及实现

从硬件的角度看,以太网接口电路主要由 MAC 控制器和物理层接口(Physical Layer, PHY)两大部分构成。S3C4510B 作为一款优秀的网络控制器,内嵌一个以太网控制器,支持媒体独立接口(MII)和带缓冲的 DMA 接口(Buffered DMA Interface, BDI)。可在半双工或全双工模式下提供 10Mbps/100Mbps 的以太网接入。在半双工模式下,控制器支持 CSMA/CD 协议,在全双工模式下支持 IEEE802.3 MAC 控制层协议。



RTL8019 的数据总线 SD[0...15]与 S3C4510B 的数据总线 XDATA[0...15] 直接相连;因为 RTL8019AS 内部寄存器的地址范围为 0x00 到 0x0F,其数据读写端口为 0x10,因此,只要有 5 根地址线就可以访问所有的内部寄存器和数据端口,所以在本系统的硬件连接中,RTL8019AS 的地址总线 SA[0...4]与 S3C4510B 的地址总线 ADDR[0...4]相连;IORB,IOWB 为读写信号线,与 S3C4510B 的 nOE,nWBE0 读写使能端相连;地址使能 AEN 端与 S3C4510B 的片选信号线 nECS1 相连;芯片的外部 I/O 脚 TPIN±,TPOUT±通过耦合隔离变压器接入 RJ45,实现与以太网的物理连接。

3 UART 接口硬件设计及实现

S3C4510B 的 UART 单元提供两个独立的异步串行 I/O 口(Asynchronous Serial I/O,SIO),每个通信口均可工作中断模式或 DMA 模式,也即 UART 能产生内部中断请求或 DMA 请求在 CPU 和串行 I/O 口之间传送数据。

RS-232-C 标准是异步串行通信中应用最广的标准总线,采用的接口是 9 芯或 25 芯的 D 型插头,以 9 芯插头为例,要完成最基本的串行通信功能,只需要其中的 RXD、TXD 和 GND 管脚即可,但由于 RS-232-C 标准所定义的高、低电平信号与 S3C4510B 系统的 LVTTTL 电路所定义的高、低电平信号完全不同,则两者之间进行通信必须经过信号电平转换,目前常使用的电平转换电路为 MAX232、MAX3232 等。

在本系统中,串口的主要作用是在需要时为系统配置 IP 地址、MAC 地址等参数,且考虑到成本、电路板面积等因素,只设计了一个 9 芯的 D 型插头,选用 S3C4510B 的 UART0,同时设计数据发送与接收的状态指示 LED,当有数据通过串口传输时,LED 闪烁,便于掌握其工作状态以及进行软、硬件调试。系统的实际电路连接如图 7。

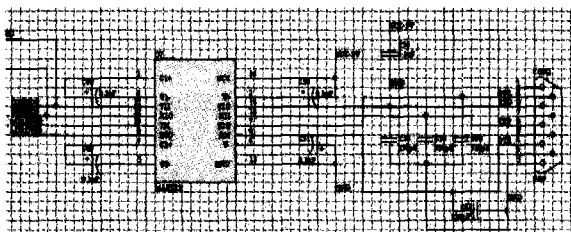


图 7 UART 电路图

4 系统 BootLoader 设计与实现

嵌入式系统中的 BootLoader 相当于 PC 机上的 BIOS,通过 BootLoader 可以完成对系统板上的主要部件如 CPU、SDRAM、Flash、串口等的初始化。在本嵌入式网关系统中,BootLoader 被烧写到 Flash 的 0x0 地址,其核心功能是完成存储器映射,地址配置,初始化串口,从 Flash 装载 uCLinux 核到 SDRAM 运行,BootLoader 程序流程如图 8。

第一次存储器映射,初始化 SDRAM 代码如下,

```
LDR R1, =0x3FF0000 ;系统配置寄存器
LDR R0, =0xE7FFFF90
STR R0, [R1]
LDR r0, =0x3FF3010
LDR r1, =0x00103000 ;外部 I/O Bank0 配置为 8 位,其他禁;
;用;SDRAM Bank0 配置为 32 位,其他;Bank 禁用)
LDR r2, =0x04000060
;Flash 配置地址为
;0x0~0x00400000-1,大小 4MB
LDR r3, =rROMCON1
LDR r4, =rROMCON2
```

```
LDR r5, =rROMCON3
LDR r6, =rROMCON4
LDR r7, =rROMCON5
LDR r8, =0x14010380 ;SDRAM 配置地址为;0x00400000~
0x1400000-1,大小 16MB
LDR r9, =rSDRAMCON1
LDR r10, =rSDRAMCON2
LDR r11, =rSDRAMCON3
LDR r12, =rSREFEXTCON
STMIA r0, {r1-r12}
```

将 Flash 的内容全部复制到 SDRAM 中,

```
LDR r0, =0x0;Flash 起始地址
LDR r1, =0x400000;复制的数据量,
;共 4MB
LDR r2, =0x400000;SDRAM 的起始地址
COPY
LDR r3, [r0], #4
STR r3, [r2], #4
SUBS r1, r1, #4
BNE COPY;按照字节复制
```

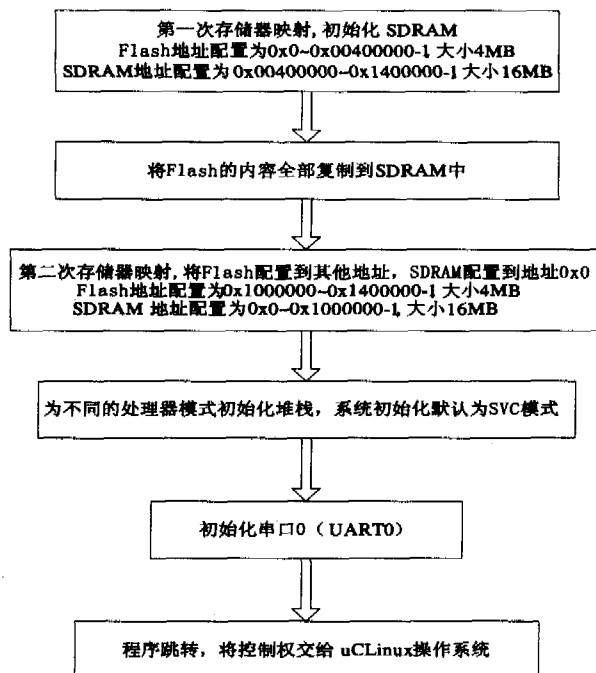


图 8 BootLoader 程序流程图

第二次存储器映射,将 Flash 配置到 0x1000000,SDRAM 配置到 0x0,

```
LDR r0, =0x3FF3010
LDR r1, =0x00103000
LDR r2, =0x14040060
;Flash 配置地址为
;0x1000000~0x1400000-1,大小 4MB
LDR r3, =rROMCON1
LDR r4, =rROMCON2
LDR r5, =rROMCON3
LDR r6, =rROMCON4
LDR r7, =rROMCON5
LDR r8, =0x10000380
;SDRAM 配置地址为 0x0~0x1000000-1,
;大小 16MB
LDR r9, =rSDRAMCON1
LDR r10, =rSDRAMCON2
LDR r11, =rSDRAMCON3
LDR r12, =rSREFEXTCON
STMIA r0, {r1-r12}
```

为不同的处理器模式初始化堆栈,系统初始化时默认为 SVC 模式,以 IRQ 模式为例设置堆栈,

```
MOV sp, #0x80000;将 SVC 堆栈设置
;在 SDRAM 的 0x80000 处
MOV r0, #0x12;切换到 IRQ 模式;并设置堆栈
MSR cpsr-c, r0 ;c 表示只改变
;CPAR 的控制位
MOV sp, #0x70000
```

(下转第 123 页)

对本方案进行攻击。他可以在秘密分发过程的第(2.2)步中,或在秘密重构过程的第(1)步中,根据各参与者 P_i 提交的信息 $V_{d_i}(r,1) \bmod N$ 或 $V_{d_i}(V_{d_i}(r,1),1) \bmod N$ 来推导出参与者 P_i 的私钥,即参与者 P_i 的秘密份额。由于 LUC 密码体制的安全性,攻击者的这种攻击无法奏效。同样道理,攻击者通过推导秘密分发者的私钥以进行模仿秘密分发者的攻击也是不可能的。

(4)由 Lagrange 插值多项式的性质^[2]可知,在秘密重构过程中,要重构一次多项式 $f(x)$ 需要知道两个满足 $Y_i = f(X_i)$ 的不同的点 (X_i, Y_i) 。利用公开信息只可以得到一个点 $(1, f(1))$ 。对于授权子集 γ_i 来说,其参与者的合作可以很容易地得到另外一个点 $(d_i, f(d_i))$;而非授权子集上参与者的合作不能得到这样的点。如果一个非授权子集 $\bar{\gamma}_i$ 上的参与者或者攻击者想要得到点 $(d_i, f(d_i))$,需要设法得到 γ_i 上任何一个参与者 P_{ij} 所提供的子秘密 $V_{d_{ij}}(V_{d_i}(r,1),1) \bmod N$,否则只能凭猜测来得到点 $(d_i, f(d_i))$ 。而要对 $f(d_i)$ 进行猜测,其成功的概率仅为 $1/Q$ 。当 Q 足够大时,这种攻击的成功概率接近于 0。

(5)该方案也是一个多重秘密共享方案^[8],可使一群参与者利用他们各自的私钥共享任意多个秘密而不必更新他们的私钥。为了共享多个秘密 $s_1, s_2, \dots, s_k \in Z_Q$,秘密分发者在进行秘密分发时,只需在秘密分发过程的第(1)步为每个秘密 $s_i (i=1,2,\dots,k)$ 随机选取一个唯一的整数 r_i 。由 LUC 密码体制的安全性可知,在秘密的分发和重构过程中,每个参与者 P_i 的私钥不会被其它参与者或系统外的任何人计算出来。而且,即使知道某个参与者 P_i 关于若干个秘密的伪份额,也不可能计算出他的关于其它秘密的伪份额。这也是本文方案的一个优点,即秘密分发者可以动态地在 n 个参与者中共享任意秘密。

(6)值得注意的是,尽管 LUC 和 RSA^[9] 通常是可替换的^[6],但是在本文的方案中不可以使用 RSA 来替换 LUC,这种替换会导致方案安全性的降低。这是因为在 RSA 体制中,数字签字的乘积是相应消息之积的数字签字,这使得 RSA 会受到公共模以及称之为自适应选择消息伪造的密码攻击^[6];而 LUC 不具有这样的乘积性质,因而不受这些攻击^[6]。这也从另一个侧面显示了本文方案的安全性。

(7)最后,需要讨论一下方案的性能。在 Shamir 的门限方案^[2]及其基于 Shamir 的方案中,如文[1,8]等,最耗时的操作为多项式插值计算。一般来说,这些方案的性能主要决定于多项式插值操作。多项式的次数越高,插值运算越复杂。

现有基于 Shamir 的方案中,采用的 Lagrange 插值多项式大多是高次多项式。目前有效的多项式插值运算的算法复杂度也仅为 $O(n \log^2 n)$ ^[1],因而这些方案效率不是很高。而在本文方案中,所采用的 Lagrange 插值多项式仅为一次多项式,多项式的构造仅需要 3 次乘(除)法和 3 次加(减)法,见式(4)。可见,本文方案比起其它基于 Shamir 的方案更为有效,而且容易实现。

结论 提出了一个基于 LUC 的一般访问结构上的秘密共享方案。参与者的秘密份额为他们的私钥,即使秘密分发者也不能获得每个参与者的秘密份额;秘密分发者和各参与者间所有的消息都可以以明文形式发送,不需要在他们之间维护一条安全信道,这对于秘密分发者与参与者之间不存在安全通信信道时的场合尤为有用;秘密重构过程中,任何人都可以立即检验每个合作的参与者是否进行了欺骗。利用该方案可以共享任意多个秘密,而不必修改参与者的秘密份额。只要 LUC 算法和 Shamir 的门限方案具有足够强的安全性,本文方案就具有很强的防欺诈、防攻击能力。

参考文献

- 1 Hwang R J, Chang C C. An on-line secret sharing scheme for multi-secrets[J]. Computer Communications, 1998, 21(13): 1170~1176
- 2 Shamir A. How to share a secret [J]. Communications of the ACM, 1979, 22(11): 612~613
- 3 Blakley G. Safeguarding cryptographic keys [A]. In: Proc. AFIPS 1979 Natl Conf [C], New York: AFIPS press, 1979. 313~317
- 4 Benaloh J, Leichter J. Generalized secret sharing and monotone functions [A]. In: Advances in Cryptology-Crypto'88 [C], Berlin: Springer-Verlag, 1990. 27~35
- 5 Wang S J. Direct construction of a secret in generalized group-oriented cryptography [J]. Computer Standards & Interface, 2004, 26(5): 455~460
- 6 Smith P. LUC public-key encryption: A secure alternative to RSA [J]. Dr. Dobbs' Journal, 1993, 18(1): 44~49
- 7 王育民,刘建伟. 通信网的安全——理论与技术[M]. 西安:西安电子科技大学出版社,1999
- 8 Yang Chou-Chen, Chang Ting-Yi, Hwang Min-Shiang. A (t, n) multi-secret sharing scheme [J]. Applied Mathematics and Computation, 2004, 151(2): 483~490
- 9 Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public key cryptosystem [J]. Communication of ACM, 1978, 21(2): 120~126

(上接第 97 页)

初始化串口,本系统选用的是 UART0,以便在系统启动时可通过超级终端查看由串口打印输出的启动信息,方便检查运行情况和调试,

```
#define ULCON0 (*(volatile unsigned *) 0x3FFD000)
#define UCON0 (*(volatile unsigned *) 0x3FFD004)
#define UBRDIV0 (*(volatile unsigned *) 0x3FFD014)
void InitUART(int Baudrate)
{
    ULCON0 = 0x03; //8 位数据,1 位停止,无校验
    UCON0 = 0x09; //当有数据读/写 UART
    //读/写 Buffer 时产生中断请求
    UBRDIV0 = Baudrate; //通过函数参数设
    //置波特率
}
```

程序跳转,控制权交给 uLinux 操作系统。在本系统中,将 uLinux 内核烧写至 Flash 起始地址为 0x8000 的存储

空间中。通过 Flash 拷贝,两次内存映射,内核起始地址被映射到 0x8000 的 SDRAM 中,因此代码为

```
LDR R0, =0x8000
MOV PC, R0
```

结束语 本系统的基本功能已设计完成,并在实验室内部测试成功,可替代原服务器充当网关。下一步的设计内容主要是为系统增加 IDE 硬盘接口使其可作为 ftp 服务器,并在网络部分加入防火墙、流量控制等扩展功能。

参考文献

- 1 李驹光. ARM 应用系统开发详解. 清华大学出版社, 2004
- 2 庞继勇,李维英,王竞. 网络通信处理器 S3C4510B 的网口驱动设计. 单片机与嵌入式系统应用, 2004
- 3 Samsung 公司. S3C4510B 芯片手册