TMS320VC5509A 系列 DSP 的程序自举引导和加密方法

陈明义　王冠星　中南大学信息科学与工程学院

摘　要： 阐述了 TMS320VC5509A 系列 DSP 基于 I2C 方式的串行程序加载和加密方法。介绍了系统的硬件连接和自举引导的实现以及基于数据驱动的连续保护方法。

关键词： TMS320VC5509A　ATMEGA8　I2C　自举引导　程序加密

Boot Investlgation and Program Encryption of TMS320VC5509A Series DSPs

Abstract: The method of EEPROM on - line programming based on the system which author designed in introduced. The sketch map of the hardware design are given. The process of bootloader and alternation for the are discussed detailly.

Keywords: TMS320VC5509A　ATMEGA8　I2C　on - line programming　programming code encryption

0　前言

随着数字信号处理技术的快速发展，DSP(数字信号处理器)以其卓越的性能、独有的特点，成为通信、计算机、消费类电子产品等领域的基础器件，已越来越广泛地应用于各种数字信号处理系统中。若要使最终开发的系统脱离仿真器运行，必须将程序代码存储在非易失性存储器中。随着对知识产权的重视，在利用 DSP 进行产品设计时，如何保护自己的成果，防止破译者窃取，也成为设计工作的一个重要方面。本文基于 TI 公司的 TMS320VC 5509A 和 Atmel 公司的 ATMEGA8 单片机构，造一种加密体制，利用加密算法来保护 DSP 程序，详细介绍系统构建的相关硬件设计和软件实现流程。

1　TMS320VC5509A 的自举引导

1.1　TMS320VC5509A 的自举过程

TMS320VC5509A 每次上电复位后，在执行完一系列初始化(配置堆栈寄存器、关闭中断、程序临时入口、符号扩展、兼容性配置)工作后，根据预先配置的自举模式，通过固化在 ROM 内的 Bootloader 程序进行程序引导。引导模式选择是通过 4 个引脚 BOOTM[0:3]配置完成的。BOOTM 0～3 引脚分别与 GPIO 1、2、3、0 相连。在本系统中，采用 ATMEGA8 微控制器代替 I2C EEPROM 存储器完成串行引导，只需将 BOOTM[3:0]设置成 0101 即可[1]。

VC5509 I2C 模块是新增的片内集成外设，可以使 DSP 与 I2C 兼容设备通过该接口进行自举引导和数据通信。它有以下特点：兼容 Philips I2C 总线规范 V2.1；支持 bit/Byte 传输格式；支持 7b/10b 设备寻址模式；全体呼叫(generalcall)功能；支持自由数据传输格式(free Data Format)；支持多 M/S 工作模式；I2C 数据传输率为 10～400 kbps；可产生 1 个读和 1 个写 DMA 同步事件，并发送给 DMA 控制器。

I2C 模块接口由串行数据信号 SDA 和串行时钟信号 SCL 组成。SDA 和 SCL 均为双向接口。VC5509 I2C 设备寄存器占用 0x3C00～0x3C0F 的 I/O 地址，通过配置可以作为主/从设备(Master/Slav-

er)发送或接收同步信号和数据。要实现 I2C 模块的启动及其在数据传输中的控制,需要对模块中的内存映射控制寄存器进行配置。配置操作主要包括两个方面:

(1)I2C 模块的初始化,包括对 ICPSC(预分频率控制寄存器)、ICCL KH 和 ICCL KL(时钟控制寄存器)以及 ICSAR(从地址寄存器)的操作,为主/从设备在总线上的数据通信做好准备[2]。

(2)I2C 通过设置 ICMDR(模式寄存器)的相关状态位,确定 I2C 工作模式。

在引导和整个程序运行过程中,VC5509A 作为主设备,ATMEGA8 微控制器作为从设备。第一次引导由固化在 ROM 内的 Bootloader 程序完成;第二次引导由用户编写的特定程序完成。

1.2 TMS320VC5509A 的引导表

Bootloader 在引导程序时,程序代码是以引导表格形式加载的。TMS320VC5509A 的引导表结构中包括了用户程序的代码段和数据段以及相应段在内存中的指定存储位置,还包括了程序入口地址、部分寄存器的配置值、可编程延时时间等信息[3],如表 1 所示。

表 1　TMS320VC5509AX 引导表结构

32 - bit 程序入口地址			
32 - bit 寄存器配置数目			
16 - bit 寄存器地址		16 - bit 寄存器内容	
16 - bit 延时标志		16 - bit 延时长度	
32 - bit 段长度(字节数) +			
32 - bit 段启始地址			
数据	数据	数据	数据
数据	数据	数据	数据
32 - bit 全零(引导表结束标志)			

在表 1 中,程序入口地址是引导表加载结束后,用户程序开始执行的地址;寄存器配置数目决定了后面有多少个寄存器需要配置。只有当延时标志为 0xFFFF 时,延时才被执行。延时长度决定了在寄存器配置后延时多少个 CPU 周期才进行下一个动作。段长度、段起始地址和数据则为用户程序中定义的各个段的内容,并且可以重复添加,最后以 0x00000000(32 个 0)作为引导表的结束标志。

若要生成引导表,可用 CCS 最终编译生成的 .out文件通过 CCS 自带的 hex55. exe 转换程序得到。将 hex55. exe、. out文件、. 0cmd 文件放在同一个文件夹中,通过 DOS 命令调用 hex55. exe,即可完成. out文件到 hex 格式的引导表文件的转化。. CMD 文件用于提供引导表的相关配置信息。以下为一个. CMD 文件的实例:

```
-boot;  说明创建 boot 文件
-v5510:2;  生成 55X boot 文件格式
-serial8;  使用串行加载方式
-reg_config 0x1c00,0x2108;  在地址 0x1C00 的寄存器写入 0x2108,配置 CPU 时钟
-delay 0x100;  延时 0x100 个 CPU 时钟周期
-i;  Hex 格式
-o Test. hex;  输出. hex 文件
-Test . out;  输入的. out文件
```

2 自举和加解密实现

2.1 TMS320VC5509A 和 ATMEGA8 的硬件设计

ATMEGA8 是一款基于 AVR 增强型 RISC 结构的低功耗 8 位 CMOS 微控制器,自带 8 kByte 字节的可编程 Flash,支持 M/S 工作模式的 I2C 数据接口,工作电压 2.7 ~ 5.5 V[4]。基于上述特性,ATMEGA8 非常适合替代 I2C EEPROM 存储器完成常规的第一次引导过程。

鉴于 ATMEGA8 自带的 Flash 较小,而使用其他大容量 Flash 的 ATMEGA 系列芯片价格较为昂贵,因此本系统选用扩展存储器(此处使用 AT24LCXX),用于存储已经加密过的最终 DSP 程序代码。硬件结构图如图 1 所示。

2.2 二次引导技术

所谓二次引导,就是通过 DSP 内部 ROM 固化的 Boot loader,引导用户自行编写一个引导程序,其功能和 ROM 固化的 Bootloader 相同,但增加了对程序代码解密的过程,并在加载结束后,把 PC 值置为新的程序入口地址。具体实现框图如图 2 所示。

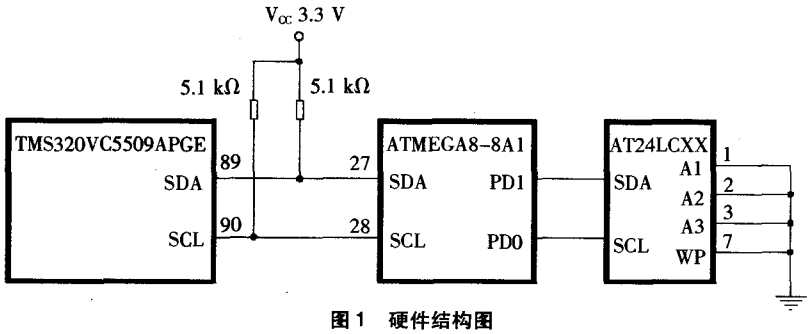

图1　硬件结构图

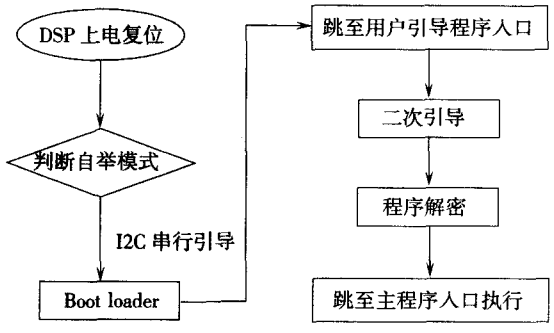

图2　二次引导及解密框图

2.3　程序加密与解密

(1)对程序的初始保护,即把最终运行的程序代码写入 AT24LCXX 芯片之前,对源代码进行加密处理。这样,AT24LCXX 中就不存在明文形式的源代码。DSP 的一次引导过程只加载储存在 ATMEGA8 中的解密程序,二次引导则加载 AT24LCXX 中已经加密的源代码,然后从 ATMEGA8 中取出密钥进行解密,加载结束和完成解密后再继续运行。由于只使用到 1 个密钥,破译者可以通过物理方式捕获 DSP 和 ATMEGA8 之间的通信数据,很容易地得到密钥和解密算法。

(2)基于数据驱动的连续保护。它的处理对象是一些重要参数或变量,通过"加锁",让它们一直以密文形式存在于程序中。只有需要使用这些数据时,才从 ATMEGA8 中取出密钥进行解密;使用结束后,仍旧"加锁"保护,使之仍然是密文形式。此时 ATMEGA8 中密钥的生成必须和 DSP 主程序中的加密处理"同步",即主程序的加密密钥要和 ATMEGA8 内生成的对应密钥相同,这可以由 DSP 监控程序利用 DSP 内部的中断程序协调实现。使用密钥 Ki 对某参数或变量加密结束后,通过中断告诉监控程序加密完成,然后锁毁该密钥。继续执行 DSP 程序时,若需要使用该参数或变量,就向监控程序发出要求,在监控程序的控制下,从 ATMEGA8 中取出对应密钥 Ki,解密。

加入连续保护后,破译者要想获得源代码,必须跟踪程序的整个运行过程。这样,对于破译者而言,所花费的代价等于自己独立写一套程序,显然也失去了破译的必要。

(3)对于 DSP 源代码加密,可以利用 3DES、Geffe 发生器和 MD5 等算法,并根据 DSP 运行闲余机时选择密钥个数和加密复杂程度。具体应用可以参考相关资料。

3　结语

本文阐述了一种针对 TMS320VC5509A 系列 DSP,使用 I2C 方式实现程序自举引导的方式;并提出基于该方式的程序加密方法。在此后的 DSP 程序升级过程中,只需要更新 AT24LCXX 内部已经加密程序,就可以通过拔下 AT24LCXX 芯片放入编程器更新;也可以编写专用上位机软件,通过 ATMEGA8 的串口实现 AT24LCXX 程序更新。这样,对产品的软件升级和保护设计成果具有积极意义。

参　考　文　献

[1] Texas Instruments. TMS320VC55x DSP CPU Reference Guide[N]. Texas Instruments,2004.

[2] Texas Instruments. Programming the TMS320VC5509 I2C Peripheral[N]. Texas Instruments,2004.

[3] Texas Instruments. Using the TMS320VC5503/VC-5507/VC5509/VC5509A Bootloader[N]. Texas Instruments,2004.

[4] Atmel Corporation. ATmega8 Data Sheet[N]. Atmel Corporation, 2004.