DOI:10.15923/j.cnki.cn22-1382/t.2017.4.04

一种 51 系列单片机的解密方法

李会杰[1]， 李俊廷[1*]， 张 伟[2]， 李严军[2]

(1.长春工业大学 机电工程学院，吉林 长春 130012；
2.长春工业大学 电气与电子工程学院，吉林 长春 130012)

摘 要： 通过控制 EA 的电平，先使单片机执行外部存储器中的程序，在片外存储器中执行跳转指令跳转到超出片内程序存储器地址的执行程序时，将 EA 改为低电平，用指令读取片内地址范围的目标码。单片机通过串口将目标码发送到上位机，从而实现解码。本解密方法也适用于具有最小模式和微处理器模式的 DSP 及 ARM 的解密。

关键词： 51 系列单片机；数据存储器；程序存储器；解密

中图分类号： TP 309.7 **文献标志码：** A **文章编号：** 1674-1374(2017)04-0335-05

A method for decrypting 51 series microcontroller

LI Huijie[1]， LI Junting[1*]， ZHANG Wei[2]， LI Yanjun[2]

(1.School of Mechatronic Engineering, Changchun University of Technology, Changchun 130012, China;
2.School of Electrical & Electronic Engineering, Changchun University of Technology, Changchun 130012, China)

Abstract: By controlling EA level in the 51 series microcontroller, external program is run first. When external ROM jumps to the program as internal ROM address rangeis exceeded, with a jump command, EA level is changed to low. Then the code in internal ROM is read and sent to the host computer through serial port, and the decryption is realized. The method is also applicable to DSP or ARM microprocessor with minimum mode and microprocessor mode.

Key words: 51 series microcontroller; data memory; program memory; decryption.

0 引 言

51 单片机在工业控制系统中广泛流行，企业为了防止 51 单片机内部程序资料外泄，进行了加密。这种加密虽然防止了对 51 单片机内部程序资料的外泄，同时也存在缺点[1]。如果企业丢失原有 51 单片机的内部程序资料，则资料无法找回，从而给企业的生产造成了严重的损失。文中提出一种 51 单片机的解密方法，同时也适用于具有最小模式和微处理器模式的 DSP 和 ARM 的解密，为了方便企业找回丢失的单片机内部资料，减少企业因丢失内部资料而带来的损失。

收稿日期： 2017-03-21
基金项目： 长春市科技计划基金资助项目(13KG09)
作者简介： 李会杰(1965—)，女，汉族，吉林九台人，长春工业大学副教授，硕士，主要从事机电一体化方向研究，E-mail:710383958@qq.com. *通讯作者：李俊廷(1990—)，男，汉族，吉林磐石人，长春工业大学硕士研究生，主要从事机电一体化方向研究，E-mail:1758904374@qq.com.

通过研究分析51单片机的程序存储器和数据存储器的结构与功能，提出了一种针对51单片机和具有最小模式以及微处理器模式的DSP和ARM的解密方式。

1 51系列单片机存储器的结构特点

程序存储器和数据存储器分开设置，并且具有各自的寻址机构和寻址方式的这种结构特点是51系列单片机的特色[2]。标准的51单片机具有128 B的片内数据存储器、4 KB(对于52是8 KB)的片内程序存储器。51系列单片机的存储器组织结构如图1所示。

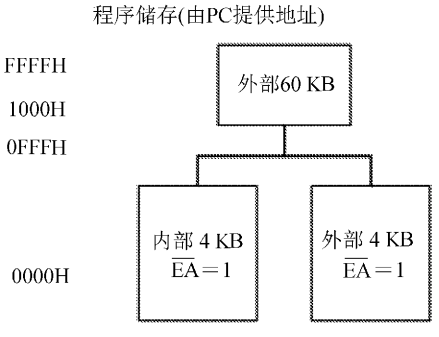

图1 程序存储器映射关系

片内程序存储器和片外程序存储器、片内数据存储器和片外数据存储器分别是51系列单片机的4个物理存储空间；片内程序存储器和片外程序存储器是统一编制的，单片机的控制器通过一个控制引脚EA用来区分内部程序存储器和外部程序存储器[3]。当EA接高电平时，单片机从片内程序存储器区取指令，内部程序地址容量小于指令地址时，自动地转向片外程序存储器取指令；当EA接低电平时，尽管内部存储器内有程序单片机也不会执行，这时单片机只能从片外程序存储器读取指令[4]。这种接法只用于采用8031单片机的场合，由于8031内部不带ROM，所以使用时必须EA=0，以便直接从外部ROM中取指令[5]。

所有51系列单片机程序的执行入口地址是存储器的0000H地址单元，一旦复位执行后，单片机返回到0000H地址单元重新执行程序[6]。51单片机的程序存储器或RAM的选择都是根据不同的信号来源进行分配的。通信号PSEN的选择是在从外部程序存储器取指令的情况下，对于从外部RAM读取并写录数据的情况应采用读写信号$\overline{RD}$/$\overline{WR}$来选通，因此，就不会产生因为地址重叠造成的混乱现象。

2 外部总线的扩展

51系列单片机需要扩展对外总线(局部系统总线)，原因是51系列单片机无论在执行I/O接口时，还是执行对外存储器时都要受到管脚的限制[7]。

51系列单片机的引脚ALE作为地址锁存信号来使用时，ALE高电平有效，低电平无效，ALE为高电平时作为锁存信号。ALE为高电平时51系列单片机片外扩展的地址锁存器将PO口上的地址信息锁存，地址信息锁存完毕后ALE变成电平无效不会继续地址信息锁存，直到ALE再次变为高电平[8-9]。在ALE为低电平有效期间，P0口作为数据总线口用来传送数据。这样就把P0口扩展为地址/数据总线复用。地址高8位A15～A8的输出口是P2，P2和P0口的锁存器共同组成对外16位地址总线AB15～AB0，P0口同时也作为DB7～DB0的8位数据总线。数据总线的主要作用是传送指令和数据信息。

51系列单片机的外部控制总线(CONTROLBUS，CB)是由输入控制信号线(如EA、INT0、INT1、RST、TO、T1)和输出控制信号线(RD、WR、PSEN、ALE)等共同组成的，如图2所示。

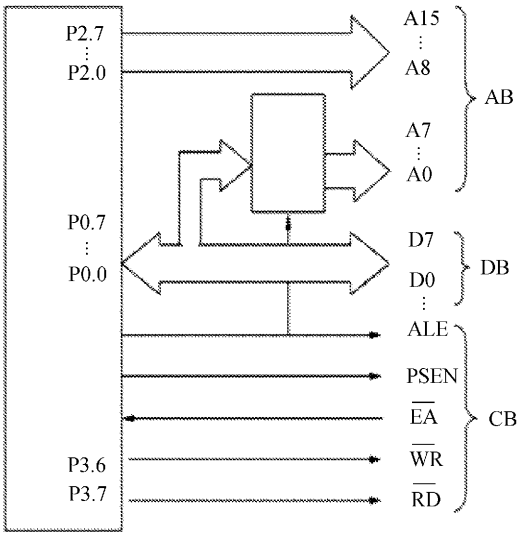

图2 51单片机的总线结构

3 解密原理

解密时的电路原理如图3所示。

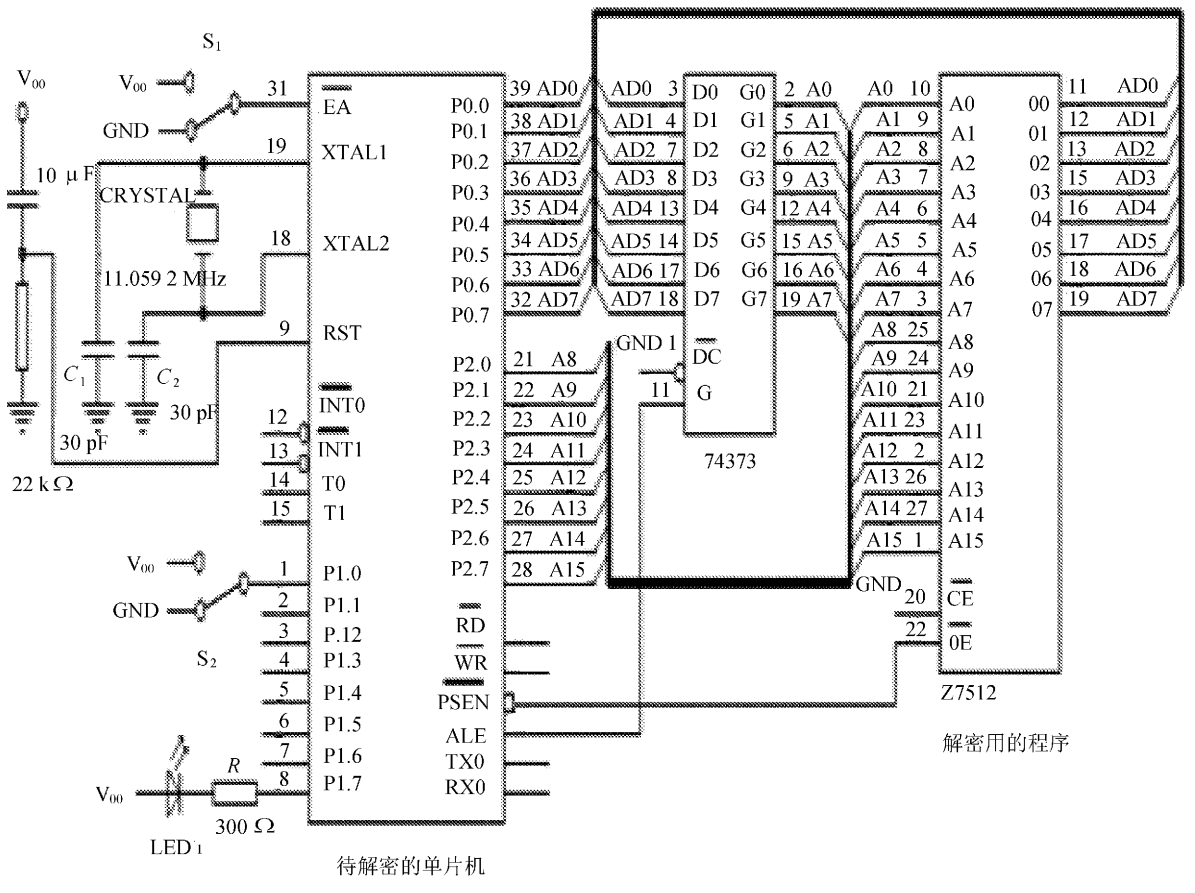

图 3　解密时使用的电路原理图

图中，上电前把 S_1 接低电平，即 EA 接通低电平，此时单片机执行片外程序存储器中的程序。片外程序存储 0000H 地址单元的是 LJMP 8000H 指令。

开始进行解密时，先从片外程序存储器开始运行程序，从 0000H 地址单元读取指令 LJMP 8000H 指令并执行后，跳转到 8000H，此时已经超出片内程序存储器的地址范围，程序自动转到片外程序存储器，与 EA 电平无关。这时使 S_1 转变成高电平状态，因程序地址超出了片内地址，虽然 EA 为高电平，但程序还是照常运行。

在片外程序存储器中存有循环检测 S_2 状态的程序，若 S_2 的状态为低电平，则不断循环检测 S_2 的状态。当 S_2 变高时，跳出上述循环，置低 P1.7 口，使得发光二极管 LED_1 点亮。因 EA 已经接高电平，此时在 8000H 以上（超出片内程序存储器地址），执行 MOVC A，@A＋DPTR 指令去读取 0～0FFFH 地址范围的程序存储器中的代码时，因 EA 是高电平读到片内程序的代码。将该代码通过串口送到电脑，即获得了所要程序的目标码，也就是实现了解密。此过程如图 4 所示。

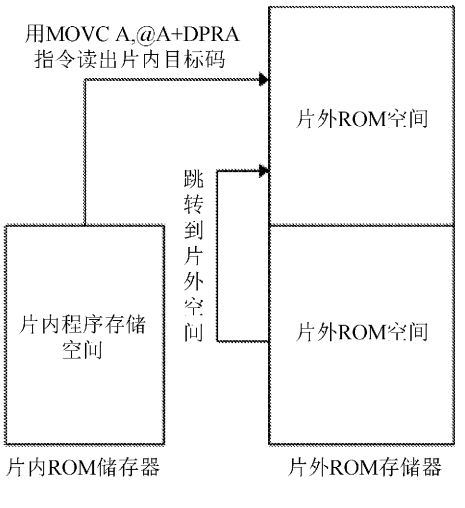

图 4　片外存储器与片内存储器的寻址顺序示意图

解密过程序的流程如图 5 所示。

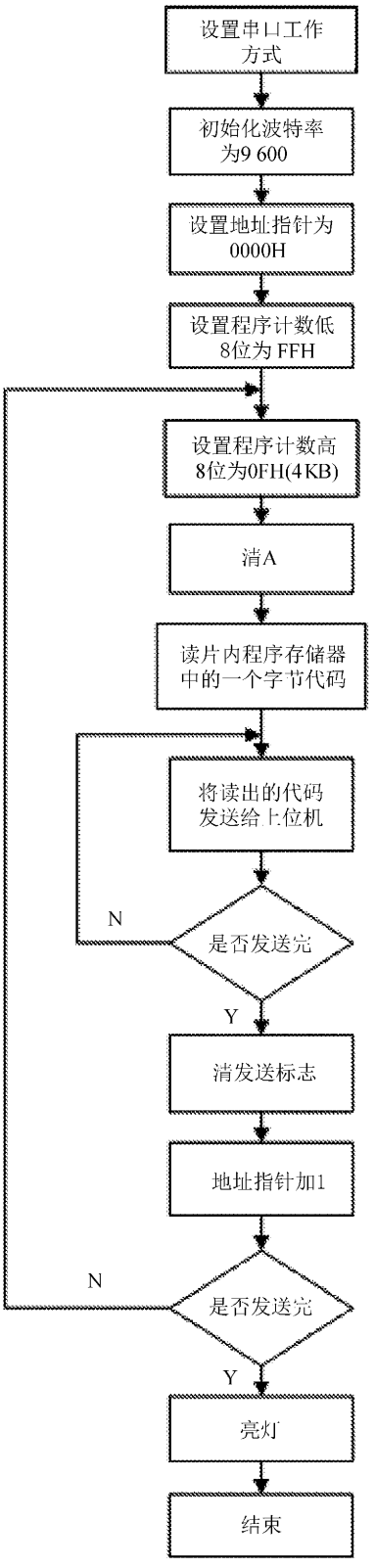

图 5 解密过程程序流程图

根据上述解密过程编制的解密程序为：

```
ORG     0000H
LJMP    8000H
ORG     8000H
    MOV     DPTR,#0000H
    MOV     R7,#0FFH
    MOV     R6,#0FH
    MOV     TCON,#20H
    MOV     TH1,#0F4H
    MOV     TL1,#0F4H
    MOV     SCON,#50H
    JNB     P1,7$
LP:CLRA
    MOVC    A,@A+DPTR
    MOV     SBUF,A
    JNB     T1,$
    CLR     T1
    INC         DPTR
    DJNZ    R7,LP
    MOV     R7,#0FFH
    DJNZ    R6,LP
    LCR     P1.7
    SJNP    $
```

4 试验结果

根据实验，通过上述的理论分析和程序解密出 51 单片机的内部程序代码的结果，如图 6 所示。

由图 6 可以看出，解密的代码将解密出的代码输入 51 单片机重新执行，执行结果和原程序的执行结果一样，说明解密的结果是成功的。文中的解密方法同样也适用于 ARM 和 DSP 等单片机。

5 结 语

基于 51 单片机的内部结构提出一种有效的解密方法，其在实验过程中运行良好，解密出的 51 内部资料没有失真，为企业方便找回内部资料有着很大的意义，并能为公司减少由于管理疏忽带来的损失。

图 6　解密试验结果

参考文献：

[1] Ninsraku W, Biolek D, Jaikla W, et al. Electronically controlled high input and low output impedance voltage mode multifunction filter with grounded capacitors[J]. AEU-International Journal of Electronics and Communications, 2014, 68(12): 1239-1246.

[2] Vellakudiyan J, Muthuchidambaranathan P, Bui F M, et al. Performance of a subcarrier intensity modulated differential phase-shift keying over generalized turbulence channel[J]. AEU-International Journal of Electronics and Communications, 2015, 69(11): 1569-1573.

[3] 葛秀梅，仲伟波.基于 DSP 的混沌语音加密解密[J]. 系统实验室研究与探索，2014，10(9)：137-140.

[4] 刘伏文，王春华. MCS-51 单片机存储器结构详解[J].电子制作，2007，32(10)：54-57.

[5] Raj J J R, Rahman S M K, Anand S. 8051 microcontroller to FPGA and ADC interface design for high speed parallel processing systems-Application in ultrasound scanners[J]. Engineering Science and Technology an International Jouranl, 2016: 1416-1423.

[6] 汪凯.基于 ARM9 和 FPGA 远程动态重构加解密研究[D].大连：大连理工大学，2014.

[7] 孙娇.基于 ARM 的文件加密技术的研究与实现[D].西安：西安电子科技大学，2015.

[8] Asbullah, Muhammad Asyrat Ariffin, Muhammad Rezal Kamel. Fast decryption method for a rabin Primitive-Basedcry ptosystem[J]. Proquest, 2014: 56-67.

[9] 安志勇，杨帆，曹秒，等.一种基于 STC 单片机和绝对式编码器的步进电机控制方法[J].长春工业大学学报：自然科学版，2013，34(1)：67-69.