数据字段伪 CRC 校验码生成技术

赵星明 （泰安山东水利专科学校 271000）

摘要：软磁盘控制器向扇区写数据时，会在写完最后一个数据字节的同时，自动生成两个字节的循环冗余校验码 CRC 并写入磁盘，正常情况下生成的 CRC 校验码是正确的，但也能人为生成错误的 CRC 校验码，形成了一种十分有效的加密技术——人为生成伪 CRC 加密法，在商品软件中得到采用。本文介绍了如何利用程序的方法生成伪 CRC 校验码并写入正确的扇区数据。

关键字：软磁盘控制器 校验码 中断控制器 定时器

一、引言

随着计算机的不断发展，一些反拷贝加密技术已公诸于众，被很多人掌握，并出现了大量的解密软件，这就要求软件开发者采用更有效的反拷贝技术以保护自己的合法权益。数据字段伪 CRC 校验码加密技术是一种有效的反拷贝技术，它利用程序的方法在扇区上产生只有磁盘有物理性的缺陷或损伤时才会产生的错误 CRC 校验码，甚至要求有正确的扇区数据，实现起来困难较大，被广泛地应用在商品软件中。本文主要介绍利用程序的方法生成伪 CRC 校验码的基本原理和方法。

二、数据字段伪 CRC 校验码生成原理

磁盘的格式化命令将每个磁道沿径向划分成若干个扇区，每个扇区中的数据域物理长度为 $128*2^n$ 个字节（n=0,1,2,3,4,5,6 为记录长度），但这并不是指整个扇区的长度，扇区中除了数据域外还有其他域。每个扇区由标识域、间隙 1、数据域、间隙 2 组成。标识域包括同步字段（SYNC）、ID 地址标志（AM1）、ID 字段和循环冗余校验码（LYCRC），数据域包括同步字段（SYNC）、数据标志（AM2）、数据字段（DATA）和校验码（CRC），两个间隙用作缓冲。图 1 为扇区的完整构成。

每个字段的内容是格式化时自动填入的，若格式化参数不变，两片软盘的同一道同一扇区的每个字段的内容是一样的。每个扇区的第一个 SYNC 用于读 ID 场的同步，第二个 SYNC 用于读数据场的同步。软盘控制器是从数据场的 SYNC 开始写扇区数据的，当写完数据后自动生成两个字节的循环冗余校验码 CRC 并同时写入数据域之后。正常的数据写入产生的 CRC 校验码是正确的，除非软盘有物理性缺陷或损伤，否则本身绝对不会产生错误的 CRC 校验码，因而利用传统的复制工具复制经过此种加密方法处理的软磁盘，肯定不能复制人为生成的错误的 CRC 校验码。当被加密程序运行时，首先利用在被加密程序中安排的一段程序对磁盘磁道的特定扇区进行检查，如果发现特定扇区中有错误的 CRC 校验码，则认为此磁盘是原盘；如果发现特定扇区中没有错误的 CRC 校验码，则认为此磁盘是复制盘，并作异常处理。

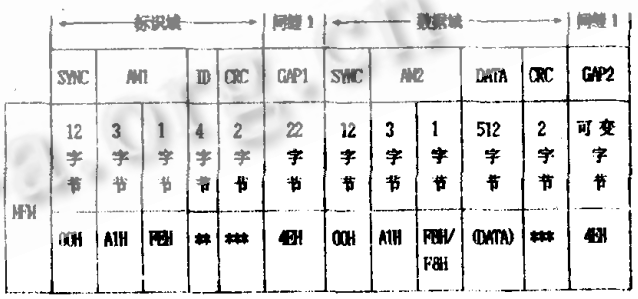

图 1

如何人为地编制程序，在数据写入软盘时，人为地产生数据字段的错误的 CRC 校验码呢？这就要求当软盘正在进行数据的写入，并且恰恰是在磁道的某一扇区数据写入过程已经开始，但还没有结束时，人为地在适当的时刻复位软磁盘控制器，从而打断了磁盘的数据写入过程，导致数据写入的混乱，从而产生数据字段的错误 CRC 校验码，人为地生成了伪 CRC 校验码。只是生成错

误的 CRC 校验码而不管扇区数据是否正确，实现起来要容易些。若既要保证数据的准确又要产生错误的 CRC 校验码，就只能控制软磁盘控制器在正写入两个字节数据字段 CRC 校验码的那一瞬间复位软磁盘控制器。若在 CRC 校验码写入之后复位就不会产生错误的 CRC 校验码，若在 CRC 校验码写入之前复位就会使扇区数据变形保证不了数据的准确性。因此数据字段伪 CRC 校验码生成技术还必须用 8253 定时器和 8237 中的 DMA 通道 2 当前字节计数寄存器才能实现。

8253 定时器主要完成各种不同的定时操作和计数功能，它有 3 个定时通道，能够同时完成特定的定时和计数。在实际编程中只对通道 0 进行编程。通道 0 在系统加电时就被 BIOS 初始化，并以时钟输入端为方波的方式和计数为 0000H 开始计数，一直累加到下个 0000H 之前共计数 65535 次，因此，通道 0 的输出频率为 = 1.19318MHz/65536 = 18.2Hz。此时若中断允许的话(即 08H 号中断)，以每秒将有 18.2 次的中断发生或者以 55 毫秒的时间间隔进行中断，编程中可以修改通道 0，减小中断间隔时间，加快时钟步伐。

DMA 控制逻辑通常采用高性能的可编程直接存储器访问控制器(DMAC)8237，它有四个独立的 DMA 通道，其中通道 2 用于软盘的 DMA 操作，有 64K 地址和计数能力，且有四个 16 位的寄存器，它们分别是基地址寄存器、基字节计数寄存器、当前地址寄存器、当前字节计数寄存器。在编程中，可以每隔一个时钟中断读取通道 2 当前字节计数寄存器，监视软磁盘控制器向扇区写数据的剩余字节数，在写完最后一个字节时复位软磁盘控制器，使两字节的 CRC 校验码由于没有写完(或磁道噪声)而错误产生，由此生成了伪 CRC 校验码。

三、数据字段伪 CRC 校验码生成方法

1. 提高时钟频率

首先设置 8253 定时器的工作方式。8253 定时器有 4 种工作方式，采用何种方式取决于对命令寄存器的控制使用，命令寄存器是一个 8 位寄存器，其 I/O 地址为 43H。

然后修改通道 0，修改输出频率即时间间隔，把时间间隔调整为 1.1ms，提高时钟频率 50 倍。

```
{
disable();
outportb(0x43,0x36); /* 置 8253 定时器方式，产生 INT 08H 的中断请求 */
outportb(0x40,0x1e); /* 间隔 = 1.1ms 置 8253 定时器的 0 通道 */
outportb(0x40,0x05); /* 二进制递减方式.先读低 8 位，后读高 8 位 */
enable();
}
```

2. 修改时钟中断处理程序

必须编写一个新的时钟中断 08H 服务程序，在程序执行过程中，一旦定时器中断发生时，CPU 自动进入 08H 中断矢量所指的用户中断处理程序的首址，使新 08H 中断服务程序以重新设置的 1.1ms 间隔被不断调用。在新的时钟中断 08H 服务程序中，加入了一个软磁盘控制器读写扇区数据字节数的监视器，这个监视器的任务是读取通道 2 当前字节计数寄存器的数据，然后判断软磁盘控制器向扇区写数据的剩余字节数，在适当时刻复位软磁盘控制器。因为已经修改了 8253 定时器的通道 0，缩短了时间间隔，而磁盘的步进马达是靠日历钟维持的，因此还必须当时间间隔达到 55ms 才能调用原来的 08H 中断程序否则就此“中断结束”，若不这样处理，磁盘的读写将无法正常进行。

```
void interrupt newtimer(void)
{
i.ch[0] = inportb(5); /* 高字节 */
i.ch[1] = inportb(5); /* 低字节 */

if(i.ii<0x5)
{
outportb(0x3f2,1);
outportb(0x5,0xff);
outportb(0x5,0xff);
}
j++;
if(j>=0x32)
{
j=0;
(*oldtimer)();
}
else
outportb(0x20,0x20); /* 中断结束 */
```

对于中断处理程序的安装已有很多资料介绍，在此不再论述。

3. 完整的 C 语言程序

该程序(diskcrc.c)全部用 Turbo C 2.0 编写，并调试通过。

```
#include <dos.h>
#include <stdlib.h>
#define sizeprogram 0x239
void interrupt ( * oldtimer)(void);
void interrupt newtimer(void);
static union REGS rg;
register int j=0;
union char-int
{
unsigned short int ii;
unsigned char ch[2];
}i;
int main()
{
disable();
outportb(0x43,0x36);
outportb(0x40,0x1e);
outportb(0x40,0x05);
    outportb(5,0xff);
    outportb(5,0xff);
    oldtimer=getvect(0x08);
enable();
    rg.x.ax=0x3100;
    rg.x.dx=sizeprogram;
    setvect(0x08,newtimer);
    intdos(&rg,&rg);
return 0;
}

void interrupt newtimer(void)
{
i.ch[0]=inportb(5); /* 高字节 */
i.ch[1]=inportb(5); /* 低字节 */
if(i.ii<0x5)
    {
    outportb(0x3f2,1);
    outportb(0x5,0xff);
    outportb(0x5,0xff);
    }
j++;
if(j>=0x32)
    {
    j=0;
    ( * oldtimer)();
    }
else
outportb(0x20,0x20);
}
```

4. 数据写入操作步骤

首先运行 diskcrc.c 编译的 EXE 程序，然后用 DEBUG 写入扇区数据即可。

```
c:\debug w5001
-u
2C42:0100 B80103   MOV   AX,0301
2C42:0103 BB0002   MOV   BX,0200
2C42:0106 B90150   MOV   CX,5001
2C42:0109 BA0000   MOV   DX,0000
2C42:010C CD13     INT   13
2C42:010E 80FC00   CMP   AH,00
2C42:0111 74ED     JZ    0100
2C42:0113 CC       INT   3
-g=100
```

四、结语

利用数据字段伪 CRC 校验码生成技术不仅适合正常 ID 扇区而且也适合异常 ID 扇区，写入数据后再读就会返回 AH=10H,的错误代码，所需的扇区数据也会被正确写入。国内大部分商品软件都采用了这种加密技术，当然在同一张磁盘上采用多种反拷贝技术加密，其对抗性会更强。

(来稿时间:1997 年 7 月)