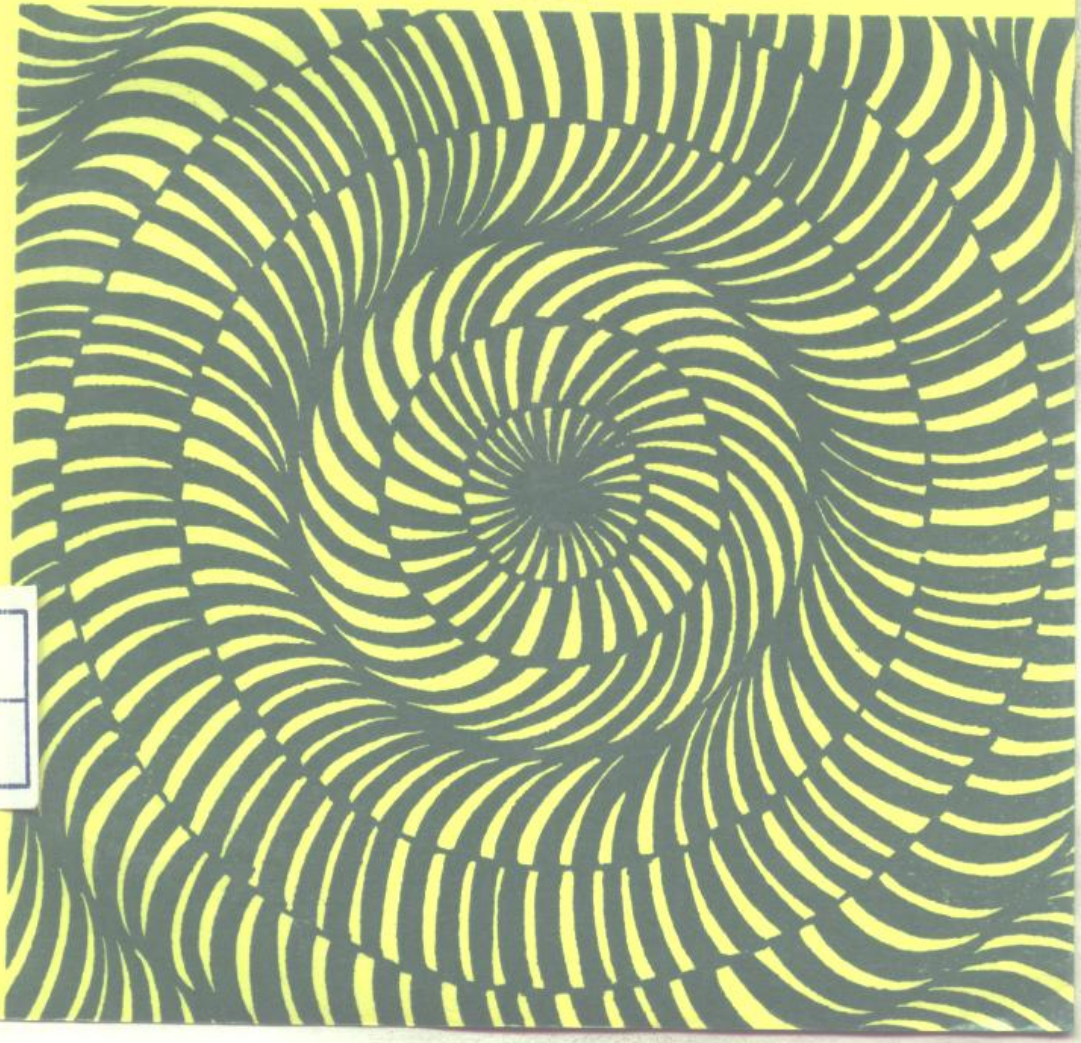
软件保护技术

周晓东　卢东明　编著

清华大学出版社



软件保护技术

周晓东　卢东明　编著

清华大学出版社

(京)新登字 158 号

图书在版编目（CIP）数据

软件保护技术/周晓东，卢东明编．—北京：清华大学出版社，1994

ISBN 7-302-01579-1

Ⅰ．软… Ⅱ．①周…②卢… Ⅲ．电子计算机-密码术 Ⅳ．TP309

中国版本图书馆 CIP 数据核字（94）第 07020 号

出版者：清华大学出版社(北京清华大学校内，邮编 100084)
印刷者：通县宏飞印刷厂
发行者：新华书店总店北京科技发行所
开　本：787×1092 1/32　印张：7　字数：163　千字
版　次：1994 年 11 月第 1 版　1994 年 11 月第 1 次印刷
书　号：ISBN 7-302-01579-1/TP・662
印　数：0001—3000
定　价：**8.50** 元

目 录

第一章

绪 论

1.1 软件权益的保护

众所周知，一套完整的计算机系统是由硬件和软件两部分组成的。没有多姿多彩的“软件世界”，计算机硬件就等于废铁一堆。软件作为一种商品，具有一定的市场价值，应当为大家所认可。然而由于软件本身具有容易被复制的特点，就容易被人通过贩卖盗版软件来牟取暴利，从而严重地损害软件开发者的权益。针对这种情况，程序员在开发软件的同时，必须考虑如何对软件进行保护，防止非法用户使用软件。而在高额利润的驱使下，必然会有人“反其道而行之”，去破解软件保护，从而造成软件保护和破解软件保护的对抗。随着现在软件价格的不断上涨和各种新技术的不断出现，这种对抗也“愈演愈烈”。可以肯定，在相当一段时间内这种斗争还将继续下去。到目前为止，还没有一种行之有效的、绝对无法攻破的软件保护技术，问题的难点就在这里。

就通过技术对软件进行保护而言，往往因条件各异，采用的办法也可能不同。缺乏一种统一的模式，某种方法对这种情况是适用的，然而对另一种情况可能不可行。所以究竟采用什么方法要具体问题具体分析。

对于软件开发者来说，软件保护是一项额外而且沉重的负担。而破解软件保护的人更需要花费大量的时间和精力。这种无休止的“对抗”没有给社会带来一点益处。不过在问题未彻底解决之前，我们还必须付出一定的精力从技术的角度来研究如何保护软件权益不被非法侵占。本书的目的就在于介绍若干实用的软件反拷贝技术，希望对大量从事软件工作的同志有些帮助。

1.2 软件保护方法的分类

现在市场上的每一份软件几乎都采用了某种方法来防止非法用户的拷贝和使用。这些方法一般可以归结为以下几种。

1. 密码加密

这种反拷贝技术是将软件全部或它的关键部分用加密方法转换为密文记录在软盘上。运行之前必须将密文解释为原来的程序或代码，否则无法运行。密码学在反拷贝技术中的应用有待开发，后面将专门介绍。在这里必须对什么叫密码先说几句话。所谓加密算法或密码实际上是一种带参数 k 的变换，将明文 m 转换为密文 c。即加密算法：

$$E: c=E_k(m)$$

k 称为密钥，E 是加密变换，解密变换 D 将密文 c 还原为明文 m，即

$$D: m=D_k(c)$$

要求任一第三方若不掌握密钥 k，就是截获密文 c 也无法从 c 得到 m，这个密钥 k 是通信双方私下商定的，密码是一种有效的通信保密技术，也可以用在软盘反拷贝上。经过密码加密的软

盘在运行时用户必须输入密钥。密钥从购买软件时所附带的说明书上获得。密码输入错误将被软件“拒之门外”。

这种方法的优点在于不存在什么兼容性的问题，允许用户随意备份程序，更不必担心使用寿命的问题。但它的缺点也很明显，即只要用户复印或抄下了密码表，也就相当于拥有了多套软件。另外每次要求用户查表输入密码对用户是十分麻烦的，会引起用户的反感。

这种加密方法的首要任务是保护密码表不被复制。早期的密码表都是由字母和数字组成的。为了防止复印机的复印，特制成白底黄字，使复印出来的结果是一页空白。但这种表看起来很费劲，有时甚至要通过滤色片才能看清，因此常使用户抱怨不已。目前又出现一种密码表的变种，即将一张图分成多个部分，各部分分别填上不同的颜色。程序进行密码输入时提供一张相同的空白图，并指定某些部分要求用户填入正确的颜色。由于彩色复印机尚不普及，因此可以较好地防止被复印。这种表的另一个好处在于一个人可以将一份由数字和字母组成的密码表敲入计算机，再打印出来，却很难仔细地去描一份复杂的图形并填上相应的颜色记号。但以上所有的方法都仅仅能稍稍地阻止复制软件的发生，并不能从根本上解决。由于很难解决好被强行拷贝的问题，所以此类程序在软件的密码检测方面做得都比较简单。通常是将输入的密码与密码表简单地比较就算了。因此也很容易被无密码表的非法用户跟踪并跳过比较部分。就目前来看，市场上流行最多的非法软件都是此类软件的“破解版”。只要随意键入密码或一按“回车键”就“万事大吉”。

由于密码加密本身的缺陷，使得使用这一方法的软件清一色都是廉价的游戏软件。虽然从商业的角度讲这不是一个有效的方法，但是从另一个方面来看，如果一个用户出于安全的目

的不希望别人使用某个软件，但又不能阻止别人使用机器，这种方法就成为了一个有效、可靠的方法。特别是将密码与程序有机地结合起来，可以从理论上达到程序保密的目的，只要你不告诉别人密码，别人就不可能使用它。

2. 磁盘加密

对于微机上的用户来说，磁盘加密的方法应该是最常见的。实际上，微机上的软件保护一出现就是在磁盘机上打主意。到现在为止，已经出现了各种各样的磁盘加密方法。从早期的异常扇区法到现在流行的弱位技术，无缝锁法等，其种类之繁多，技术更新之频繁，实在令人咋舌。最简单的办法是在软盘上作特殊的标志，我们通俗地称之为“指纹”。将指纹存在不易被拷贝的地方，运行前首先检查是否存在这个标志？否则拒绝执行。由于拷贝的盘无法拷走这标志，所以拷走的盘是无法运行的。比如打激光孔的办法曾风行一时，它在特定的位置上通过特殊的装置打一肉眼不容易看见的激光孔。孔是拷不走的，原盘在这地方写进去与读出来的结果将不符合，而拷贝的盘就没这功能。这种方法后面将讨论它，它是具有破坏性的，打过激光孔的盘不能作为它用，而且检查“指纹”的地方每次运行都要对它进行读写，所以也容易损坏。因此，打激光孔的办法也没生存多长时间便宣告失灵，攻击者通过追踪找到这个地方，将它修改跳过去就是了。可见保护软件的斗争是异常激烈的。

这里讲的磁盘加密形式是在程序运行的适当时候，提示用户插入附带的钥匙盘（Key Disk）验证正确后方可继续执行。

这种加密方法与密码加密法相比最大的改进就在于提供了“抗拷贝”的硬件介质——钥匙盘，这个盘对于一般的用户，是复制不出一张相同的钥匙盘的。除此之外，从磁盘输入密码，既

隐蔽又方便了用户。而且由于采用了磁盘输入，使得密码的概念不仅仅是用来进行验证的一些记号，它甚至可以是程序用到的一些重要数据或一段代码，这样就使那些没有钥匙盘的用户破译程序的希望化为了泡影。虽然采用磁盘加密有很多好处，但是人们在使用的过程中也发现了一些问题。其一是兼容性的问题。由于磁盘机的种类很多，功能也不尽相同，磁盘的格式也从最早的160K，180K 到了今天的 1.2M，1.44M。加上特殊制作的钥匙盘必然与标准格式有出入的地方，因此或多或少地都存在着不兼容的问题，而且随着反拷贝能力的逐渐增强，往往也会产生更多的不兼容情况。这是一个长期困扰加密制作者的问题。其二是软件寿命的问题，它取决于钥匙盘的寿命，由于每次启动软件都要用到钥匙盘，而读密码的动作一般又集中在盘上的某一磁道，因此容易造成钥匙盘的“失灵”。再加上不能备份钥匙盘，使得用户在使用这种软件的时候有些提心吊胆。软件不允许备份的做法本身未免也太“霸道”了，尽管如此，磁盘加密方法仍不失为一种物美价廉的加密方法，因而成为目前加密方法中的主流。

显而易见，磁盘加密最关键的一步就是做出防止拷贝的“钥匙盘”来。人们对这方面的研究已经做得非常深入了，并且提出了很多方法，但是，完全的照搬照抄将会是很危险的，只有从原理上去理解，从技术上去变化，才能制造出有特色、高强度的抗拷贝钥匙盘。在本书的第二章中将详细地介绍几种通用磁盘加密的方法供大家参考。

3. 软件狗加密

近几年来广为流行这种加密方法，大有取代磁盘加密的势头。其实质就是一块插在计算机并行口上的一个硬件电路，称

这个硬件为“软件狗”，顾名思义是用以保护软件的作用，它对计算机通过并行口发来的信号给出不同的反应，让计算机上的软件判断并识别它，从而实现软件的保护。用户在使用软件前必须在并行口上插好“软件狗”，然后才能正常地运行程序。

这种加密方法把原来存放在磁盘上的“指纹”移到了硬件电路中去，使得一般用户不会去试图复制它。因为分析制作一个硬件电路要比直接在软盘上进行分析要困难、费力得多。另外从软件分析的角度来看，分析软盘可以在软盘贴有“写保护”的方式下进行，可以确保原版软件的安全。而软件狗则没有“写保护”一类的措施，倒是有“全擦除”的功能，因此软件设计者往往设计一些“陷阱”，一旦确认有人跟踪分析，继而“全擦除”电路中的数据，这一点是软件破解者的最大顾忌，因为一旦数据丢失，就不可能被恢复，不但破解不可能，甚至连原先的软件也不能运行。除此之外，软盘操作伴随有明显的现象（磁盘灯亮，马达转动），而软件狗的操作则是无声无息，不能断定什么时候会有读写操作，这些也给软件狗的破解带来了极大的不便。

软件狗流行的原因并不仅仅在于破解困难，实际上，对于一些专业人员来说，破解软件狗可能要比破解软盘还容易。软件狗的优势在于它的使用。与磁盘加密相比，它具有以下四大优点：

（1）速度快，适宜多次查询。这一点使得软件可以定时或在关键部分多次查询，而不象软盘通常只在程序进入时查询一次。从而保证一份软件同时只能在一台机器上使用。而使用软盘加密的软件通常可以同时启动多个拷贝。

（2）使用时没有明显动作，使用户常常忘记它的存在给用户的使用带来了方便。

(3) 使用寿命长。正常的使用不必担心软件会突然“失灵”，且除软件狗外，其余软件部分可由用户随意备份保存，免去用户对磁盘寿命的担心。

(4) 没有兼容性的问题。由于软件狗服从并行口的标准，因此一般没有兼容性上的问题，而磁盘加密通常会使用标准以外的一些东西，再加上磁盘转速等机械上的误差，使数据的可靠性大大降低，从而出现大量困扰加密者的兼容性问题。

正因为软件狗克服了磁盘加密的很多缺陷，才使得越来越多的软件生产者看中了它。但是它本身也有缺陷，那就是软件之间的兼容问题。虽然现有的软件狗都含一进一出两个插口，允许多个软件狗串接在一起，但实际上这种串接超不过两个，否则就会出现混乱。设计者设计一进一出的目的也往往是为了适应串连打印机的需要。因此两个以上使用软件狗的软件就难以同时运行。此外要频繁地在计算机上拨插软件狗，用起来也很不方便。

在本书的第二章中详细地介绍了软件狗的制作方法，有兴趣的读者可以亲手试一试，比较一下几种加密方法之间的优劣。

4. 扩展卡加密

近几年也出现了一些专用于加密目的的扩展卡。用户必须将卡插在扩展槽中，才能运行相应的软件。也有一些加密卡与软件需用的附加卡（如汉卡，图像处理卡）做在了一块板子上，使两者合二为一，节约了成本，也方便了用户。

加密卡与上面的软件狗相比，最大的优点就是可以制作相当复杂的电路，增加硬件破解的难度。但是由于加密卡成本较高，使用也不方便，所以对原本不需要外部硬件设备的软件而言，一般并不愿意去使用它，而对于需要扩展卡支持的软件而

言，也并不愿再多一块加密卡，而更趋向于将两者合二为一的做法。

加密卡的原理与一般的扩展卡没有什么不同，它从计算机的总线上获取信号加以处理，再通过总线将结果返回计算机。一般在卡上都要存有程序所必需的加密后的数据，或是具有某种特殊功能的部分来变换主机传来的数据，成为软件运行时不可缺少的一部分。

加密卡的制作成本较高，也涉及较多的电路知识，因此在本书内加以省略。对于有兴趣的读者，只要有机会多接触这方面的工作，同时能够有较高的编制软件的能力，相信一定会制作出很好的加密卡来。

上面种种方法是到目前为止常见到的。由于它的迫切性，所以新的技术还在不断地推出，拷贝与反拷贝的斗争将继续下去。“道高一尺，魔高一丈”，可以用这样一句话来概括它。解决软件保护还涉及到法律和道德观念等，但本书仅就技术论技术。

第二章

制作软件“指纹”

从这一章开始，我们将进入软件保护这一奇妙的世界，在这里，你可以领略到人们为了实现软件保护而想到的一条条“锦囊妙计”，会为软件工作者们巧妙的编程技巧拍案叫绝。现在就请你准备好一部PC机，然后边看边做，相信在读完本书之后，你不仅会从原理上对加解密有较深的理解，还可以积累不少加解密的实用程序，为今后的工作提供方便。

在制作软件保护之前，首先明确一个概念，就是什么叫软件的“指纹”。一份合法软件为了验证自己不同于被拷贝的软件，就必须有一个唯一的且不能被拷贝下来的标记。这个标记就象人的指纹，因此常常被称为“指纹”或KEY（钥匙）。平时我们谈到的KEY DISK（钥匙盘）指的就是含有这种标记的磁盘。为了制作这样的标记，仅仅用DOS的功能调用是无法完成的，必须深入到BIOS中，并且利用操作系统中一些特点才能够制作出各种标记。下面，我们尽可能简要地介绍各种磁盘“指纹”的工作原理与步骤，并给出相应的程序清单。

2.1 磁盘“指纹”的制作

首先，让我们了解一下有关磁盘的基本知识，见图2.1。

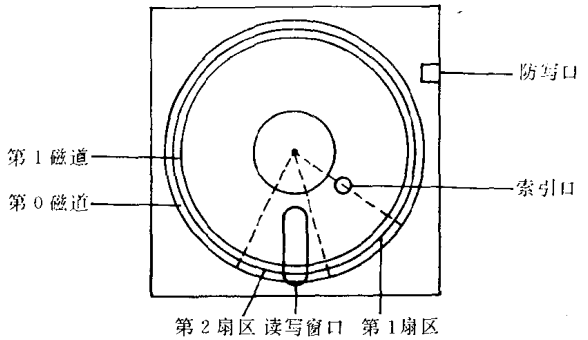


图 2.1

每张磁盘在格式化后都被分成一个个的同心圆，我们称之为磁道。磁道的计数从外到内依次增加，每个磁道上均匀地划分着数个存放数据的区域，称为扇区，扇区的大小可以调整。表 2.1 是现在常用的几种软盘格式的参数。

表 2.1

参数 \ 磁盘类型	360KB	1.2MB	720KB	1.44MB
磁头数（H）	2	2	2	2
磁道数（T）	0－39	0—79	0—79	0—79
扇区数（S）	1—9	1—15	1—9	1—18
扇区大小（N）	2	2	2	2

可由扇区的大小 N 计算出扇区的字节数 n

$n=128\times 2^N$

早期曾出现的 160K，180K 软盘（单面）现在基本上已经

不用，因此不必考虑。主要在表 2.1 上面的几种磁盘上想办法处理。

知道了磁盘的结构，还必须了解用什么对磁盘进行读写。一般说来，使用 INT 13H 调用是最简便易行的，也是最能保持软件兼容性的方法，同时又能保证制作的“指纹”有较好的防拷贝强度。当然，也有一些人直接采用端口操作的方法来控制软盘驱动电路，这种做法有利有弊，我们在 2.3 节再加以介绍。

BIOS 的 INT 13H 中有六条关于软盘的基本读写操作，现介绍如下。

1. 磁盘系统复位功能（功能号 00H）

入口参数：AH＝00H　DL＝驱动器号（00＝A，01＝B）

出口参数：无

例：

```
MOV     AH，0       ；置功能号
MOV     DL，0       ；选择 A 驱动器
INT     13H         ；磁盘复位
```

此功能是当磁盘读写功能出错时，为了再次调用此功能，应当首先调用此功能使系统重置。使用此功能时，磁盘机并不马上动作，而只是在系统中设置一标记。当启动读写功能时，若发现此标记，磁盘机会首先将磁头拉到最外面（软盘边缘）用以校准第 0 磁道，然后再执行相应的读写功能。这是常用到的一个操作。

2. 取磁盘机状态功能（功能号 01H）

入口参数：AH＝01H　DL＝驱动器号(00＝A,01＝B)

出口参数：AL＝磁盘状态　AH＝00

例：

```
MOV     AH，1       ；置功能号
MOV     DL，0       ；选择 A 驱动器
INT     13H         ；取磁盘机状态
```

此功能获取上一次读、写、验证或格式化软盘功能后的状态，它允许把错误处理或错误报告程序写成完全独立于软盘操作的部分。但对于一般软件保护的制作者来说，用处并不大，使用也不太多。

3. 读扇区功能（功能号 02H）

入口参数：AH＝02H
AL＝要读取的扇区总数
CH＝磁道号
CL＝起始扇区号
DH＝磁头（0 或 1）
DL＝磁盘机(00＝A 驱动器,01＝B 驱动器)
ES：BX＝读出数据的存放起址

出口参数：成功时：进位标志 CF＝0，AH＝0
失败时：进位标志 CF＝1，AH＝错误代码

例：

```
MOV     AX，201H     ；读取功能，长度为 1 扇区
LES     BX，BUFFER   ；数据存放在 BUFFER 中
MOV     CX，1        ；读取 0 磁道 1 扇区的内容
MOV     DX，0        ；选择 A 驱动器的磁头 0
INT     13H          ；读取数据
```

这段程序将 A 盘正面 0 道 1 扇区的内容读到用户设定的缓冲区 BUFFER 中。

此功能是验证磁盘“指纹”最重要的功能。程序通过验证