

一般解锁方法:

- 1、若知道用户原来设定的口令,可在 PC-3000AT 主菜单下按小键盘的 6 键 (或右方向键),选择“Disk security commands ---“unlock disk”,输入正确口令,回车,若提示操作成功即为解锁成功;然后,再执行 Clear password,便可完全清除用户设定的口令,此时数据无损。
- 2、若不知道用户设定的口令,但 Master password 为 \$FFFE,且 Security level 为 high,则解锁步骤同上。但输入密码时须选择 Password type: master,并输入正确的 master password。
- 3、若不知道用户设定的口令,但 Master password 为 \$FFFE,且 Security level 为 maximal,则应执行“Disk security commands -“Set password”,输入正确的 Master password,然后执行“Erase disk”。经过数十分钟的数据清除过程后,硬盘可恢复到可使用状态,但原有数据全部丢失。
- 4、若不知道用户设定的口令也不知道 Master password,则需要用特别的方法解除密码。

解开硬盘逻辑死锁的另几种有效方法(简易)

给“逻辑锁”解锁比较容易的方法是:

1. “热拔插”硬盘电源。

“热拔插”硬盘电源就是在当系统启动时,先不给被锁的硬盘加电,启动完成后在给硬盘“热插”上电源线,这样系统就可以正常控制硬盘了。这是一种非常危险的方法,为了降低危险程度,碰到“逻辑锁”后,大家最好依照下面两种比较简单和安全的方法处理。

2. ★UltraEdit ★

首先准备一张启动盘,然后在其他正常的机器上使用二进制编辑工具(推荐UltraEdit)修改软盘上的 IO.SYS 文件(修改前记住先将该文件的属性改为正常),具体是在这个文件里面搜索第一个“55AA”字符串,找到以后修改为任何其他数值即可。用这张修改过的系统软盘你就可以顺利地带着被锁的硬盘启动了。不过这时由于该硬盘正常的分区表已经被破坏,你无法用Fdisk来删除和修改分区,但是此时可以用本论坛介绍的关于分区表恢复的方法来处理。

3. ★DM ★

因为 DM 是不依赖于主板 BIOS 来识别硬盘的硬盘工具,就算在主板 BIOS 中将硬盘设为“NONE”,DM 也可识别硬盘并进行分区和格式化等操作,所以我们可以利用 DM 软件为硬盘解锁。

首先将 DM 拷到一张系统盘上,接上被锁硬盘后开机,按“Del”键进入 BIOS 设置,将所有 IDE 接口设为“NONE”并保存后退出,然后用软盘启动系统,系统即可“带锁”启动,因为此时系统根本就等于没有硬盘。

启动后运行 DM,你会发现 DM 可以识别出硬盘,选中该硬盘进行分区格式化就可以了。这种方法简单方便,但是有一个致命的缺点,就是硬盘上的数据保不住了。

硬盘逻辑锁巧解

在谈论具体的解决方法前,先讲述一下被“逻辑锁”锁住的硬盘为什么不能用普通办法启动的原因。

计算机在引导 DOS 系统时将会搜索所有逻辑盘的顺序,当 DOS 被引导时,首先要去找主引导扇区的分区表信息,位于硬盘的零头零柱面的第一个扇区的 OBEH 地址开始的地方,当分区信息开始的地方为 80H 时表示是主引导分区,其他的为扩展分区,主引导分区被定义为逻辑盘 C 盘,然后查找扩展分区的逻辑盘,被定义为 D 盘,以此类推找到 E, F, G,.... “逻辑锁”就是在此下手,修改了正常的主引导分区记录将扩展分区的第一个逻辑盘指向自己, DOS 在启动时查找到第一个逻辑盘后,查找下个逻辑盘总是找到是自己,这样一来就形成了死循环,这就是使用软驱、光驱,双硬盘都不能正常启动的原因。实际上这“逻辑锁”只是利用了 DOS 在启动时的一个小小缺陷,便令不少高手都束手无策。知道了“逻辑锁”的“上锁”原理,要解锁也就比较容易了。以前我看到有位朋友采用“热拔插”硬盘电源的方法来处理,就是在当系统启动时,先不给被锁的硬盘插上电源线,等待启动完成后在给硬盘“热插”上电源线,这时如果硬盘没有烧坏的话,系统就可以控制硬盘了。当然这是一种非常危险的方法,大家不要轻易尝试,下面介绍两种比较简单和安全的处理方法。

方法一: 修改 DOS 启动文件

首先准备一张 DOS 6.22 的系统盘,带上 debug、pctools 5.0、fdisk 等工具,然后在一台正常的机器上,使用你熟悉的二进制编辑工具(debug、pctools 5.0,或者 windows 下的 ultraedit 都行)修改软盘上的 IO.SYS 文件(修改前记住改该文件的属性为正常),具体是在这个文件里面搜索第一个“55aa”字符串,找到以后修改为任何其他数值即可。用这张修改过的系统软盘你就可以顺利地带着

[WWW.YUNWEIPC.COM/BBSXP/](http://WWW.YUNWEIPC.COM/BBSXP/) 制作: lijintim

被锁的硬盘启动了。不过这时由于该硬盘正常的分区表已经被黑客程序给恶意修改了，你无法用FDISK来删除和修改分区，而且仍无法用正常的启动盘启动系统，这时你可以用DEBUG来手工恢复。使用DEBUG手工修复硬盘步骤如下：

```
a:\>debug
-a
-xxxx:100 mov ax,0201 读一个扇区的内容
-xxxx:103 mov bx,500 设置一个缓存地址
-xxxx:106 mov cx,0001 设置第一个硬盘的硬盘指针
-xxxx:109 mov dx,0080 读零磁头
-xxxx:10c int 13 硬盘中断
-xxxx:10e int 20
-xxxx:0110 退出程序返回到指示符
-g 运行
-d500 查看运行后500地址的内容
```

这时候会发现地址6be开始的内容是硬盘分区的信息，发现此硬盘的扩展分区指向自己，这就使DOS或WINDOWS启动时查找硬盘逻辑盘进去死循环，在DEBUG指示符下用E命令修改内存数据具体如下：

```
E6BE
xx.0 xx.0 xx.0.....
.....
.....55 AA
55 AA表示硬盘有效的标记，不要修改，xx0表示把以前的数据"xx"改成0
再用硬盘中断13把修改好的数据写入硬盘就可以了，具体如下：
```

```
A:\>debug
a 100 表示修改100地址的汇编指令
-xxxx:100 mov ax,0301 写硬盘一个扇区
-xxxx: 这里直接按回车
-g 运行
-q 退出
```

然后运行FDISK/MBR(重置硬盘引导扇区的引导程序)，再重新启动电脑就行了。怎么样？用这种方法处理够简单的吧？而且这种方法还有一个好处就是可以保住盘上的数据！如果你不需要保数据的话，还有更加简单的处理方法：

方法二：巧设BIOS，用DM解锁大家知道DM软件是不依赖于主板BIOS的硬盘识别安装软件(所以在不能识别大硬盘的老主板上也可用DM来安装使用大容量硬盘)。就算在BIOS中将硬盘设为"NONE"，DM也可识别并处理硬盘。

首先你要找到和硬盘配套的DM软件(找JS要或去网上荡)，然后把DM拷到一张系统盘上。接上被锁硬盘，开机，按住DEL键，进CMOS设置，将所有IDE硬盘设为NONE(这是关键所在!)，保存设置，重启动，这时系统即可"带锁"启动。启动后运行DM，你会发现DM可以绕过BIOS，识别出硬盘，选中该硬盘，分区格式化，就OK了。这么简单？不过这种方法的弱点是硬盘上的数据将全部丢失。

### 关于硬盘解密

硬盘密码分user和master2种，加密等级有2种，高级和最高级，master密码可以解除user密码，一般的硬盘有通用master密码，如果加

user高级密码，不断电，硬盘没被锁定，可以直接重加密解除，如果断电，硬盘被锁定，拒绝读写数据区，固件区仍可以操作，如修改容量，读fw

等操作。用HDDL或pc3k的密码选项，直接输入master密码，可以解除(部分厂家的硬盘的master是空或厂家的笔记本和MHDD及HDLOCK

类加的都是user的高级密码，MHDD加的是明文HDLOCK加的是密文，如果pc3k支持这种硬盘，可以直接进入相应选项查看和清除密码，没这个选项，就读出fw，用软件修改里面的内容！

[WWW.YUNWEIPC.COM/BBSXP/](http://WWW.YUNWEIPC.COM/BBSXP/) 制作: lijintim

解开硬盘逻辑锁的有效方法

## 一、序言

不知道你是否曾碰到过从软盘和硬盘都启动不了计算机的情形?一般计算机的硬盘分区表被病毒感染后,若不能启动机器,通常从软盘可以启动。但在严重的情形下,不但从硬盘不能启动机器,就是从软盘也不能启动。有的恶毒的病毒就能使硬盘被死锁。笔者一次在自己机器上玩弄硬盘锁时,就被锁住过一次。结果在硬盘下选择DOS或WIN95模式启动机器都死机。在软盘下用DOS启动也死机。在COMS中将硬盘类型选择None,虽然可以从软盘启动,但启动后没有硬盘,使用软盘上的FDISK命令,想重新分区或格式化都没门。弄得我一筹莫展。

本来,硬盘被锁住时,可以采用3.0以下的DOS版本启动机器,机器启动后虽然也不认硬盘,但其不认的原因在于其管理不了现在的大硬盘,因此可以用Debug修改硬盘分区表,修改后可以启动。但在已进入WINDOWS的年代,3.0以下的DOS实难找到,即使找到,你的机器上恐怕也因没有5寸软驱而不能使用。因此,最好的办法是编制一个程序来解决这个问题。笔者通过尝试和思考,找到一种比较实用的方法,可以轻松解开死锁的硬盘,当然也把自己的硬盘解开了。下面,我将这种方法介绍出来。

## 二、硬盘锁住原理

硬盘锁住通常是对硬盘的分区表做手脚,因此首先应该了解硬盘的分区表。硬盘分区表位于0柱面0磁头1扇区,这个扇区的前面200多个字节是主引导程序,后面从01BEH开始的64个字节是分区表。分区表共64字节,分为4栏,每栏16字节,用来描述一个分区。如果是用DOS的FDISK程序分区后,最多只用两栏,第一栏描述基本的DOS分区,二栏描述扩展的DOS分区。分区表一栏的结构与各字节的含义如下:

00H—标志活动字节,活动DOS分区为80H,其它为00H。

01H—本分区逻辑0扇区所在的磁头号。

02H—逻辑0扇区所在柱面中的扇区号。

03H—逻辑0扇区所在的柱面号。

04H—分区类型标志。

05H—本分区最后一个扇区的磁头号。

06H—最后一个扇区的扇区号。

07H—最后一个柱面的柱面号。

08H—硬盘上在本分区之前的扇区总数,用双字表示。

0CH—本分区的扇区总数,从逻辑0扇区计数,不含隐藏扇区,用双字表示。

在上面的介绍中给出的柱面号与扇区号虽然各占一个字节,但实际上扇区号用6位表示,柱面号用10位表示,扇区号所在字节的最高两位实际上是柱面号的最高两位。分区表的最后两个字节是分区表的有效标志,如果将其改变,将不能从硬盘启动,这是一种简单的锁住硬盘的方法。解决的办法是从软盘启动,启动后硬盘仍然可以使用。用Debug或Norton中的Diskedit软件将硬盘该分区表中的标志恢复,则从硬盘启动也没有问题了。锁住硬盘的另一种方法是对分区参数做手脚,如果将分区参数全部变为0,则启动时由于找不到分区参数,从硬盘是没法启动,从软盘启动后也不认硬盘,如果你敲入盘符C并回车,将出现提示Invalid driverspecification。

但所幸的是,毕竟可以启动机器,不认硬盘没关系,在A盘上用DOS的Debug仍然可以读出硬盘0柱面0磁头1扇区的内容,修改后再写入0柱面0磁头1扇区,重新启动机器又没问题了。如果将分区表参数随意改为其它参数,则有可能不能用可以安装DOS的DOS系统盘启动,按F3退出后将出现内存分配错误,不能装载DOS的命令解释器COMMAND的提示,系统就死机了,笔者就曾碰见过这种情形。但用一张格式化系统盘的软盘则可以顺利启动,只要有Debug,你仍然可以将分区表参数修改回去。

可怕的事情是,如果你不幸将分区表参数改成一个循环链,即C盘的下一个分区指向D驱,D驱的下一个分区又指向C区,这样循环下去,DOS启动或WIN95启动时由于无休止的读取逻辑驱动器,就只有死机的份了。这是只要有硬盘存在,不管你用软盘还是硬盘都没法启动机器了,由于不能启动是由于硬盘造成的,即使你将硬盘下到其它计算机上,也没法使用,这样硬盘就彻底被锁死了,笔者所遭遇就是此情形。不信,你只需将硬盘0柱面0磁头1扇区的1D0H处改为1C。如果你的D驱开始柱面号不够大,此处本来就为1D,将1D1H处改为0,表示D驱的开始柱面号跟C盘一样。看看你的计算机还能不能启动,不过你在没有充分的准备前绝不要试。

一个完整的硬盘锁程序,不过是重新改写0柱面0磁头1扇区的引导程序,并将分区表破坏或故意制造一个循环分区表,而将真正的硬盘分区表参数和引导程序放在其它隐藏扇区并保护起来,如果启动时口令不对,则不能启动机器,口令对了则顺利启动。这种硬盘锁程序,情形好的还可以用软盘启动;情形严重的就是连软盘也不能启动,硬盘真被锁住。

---

[WWW.YUNWEIPC.COM/BBSXP/](http://WWW.YUNWEIPC.COM/BBSXP/) 制作: lijintim

希捷硬 盘加密 用汇编去除的 简易 方法。。。。

希捷硬 盘的解密:

B2000,2000

buffer 2000 comparing to 2000 RD:0000:10:00 WR:0010:10:00

Addr 0 1 2 3 4 5 6 7 8 9 A B C D E F 10 1 2 3 4 5 6 7 8 9 A B C D E F

400000 01005365 61676174 65202020 20202020 20202020 20202020 20202020

400020 20200000 00000000 00000000 00000000 00000000 00000000 00000000

400040 00000000 00000000 00000000 00000000 00000000 00000000 00000000

400060 00000000 00000000 00000000 00000000 00000000 00000000 00000000

把 前面数字部分全部 修改成 0 就可以了。。。。。。。。

[WWW.YUNWEIPC.COM/BBSXP/](http://WWW.YUNWEIPC.COM/BBSXP/) 制作: lijintim