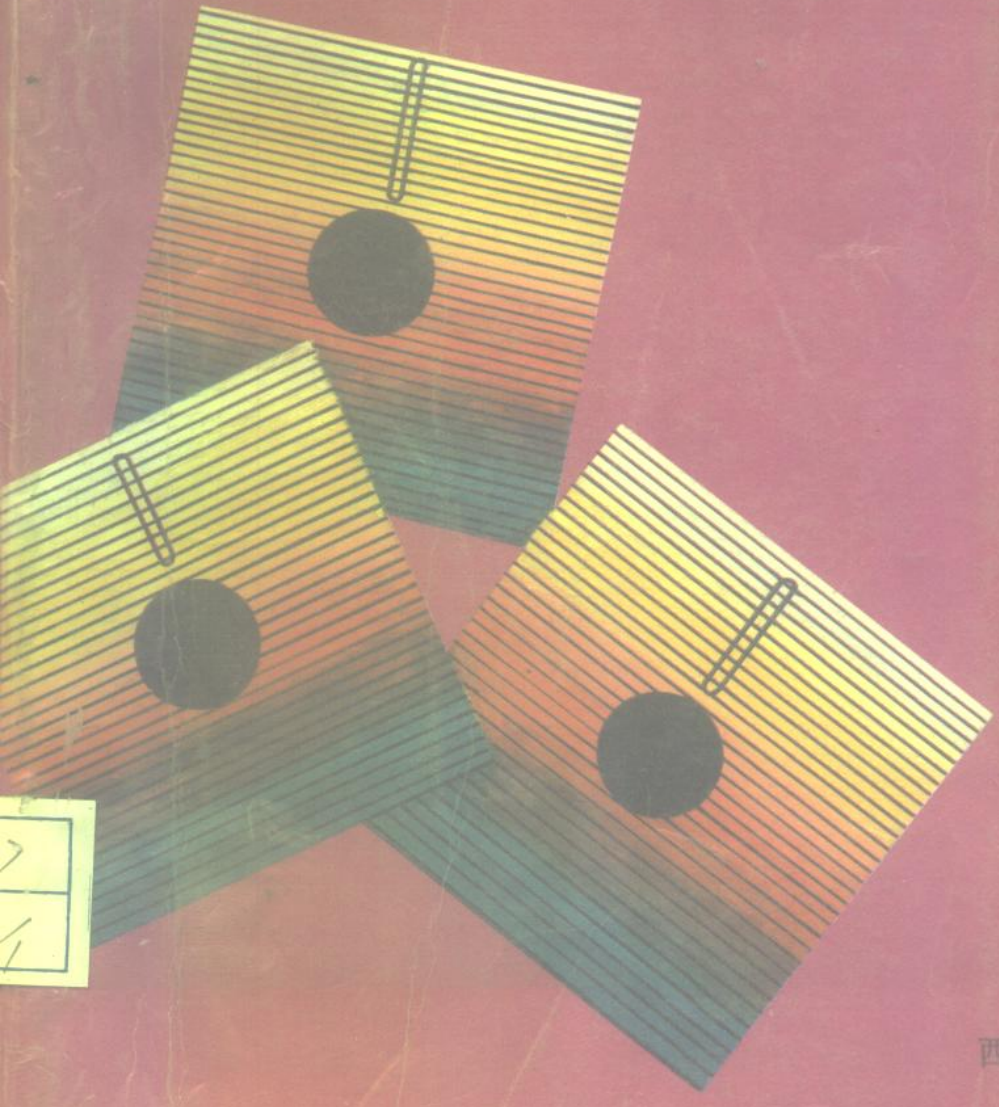
磁盘加密解密实用技术

● 林宣雄　主编
● 谭晓生　王卫东



西安交通大学出版社

磁盘加密解密实用技术

林宣雄　主编
谭晓生　王卫东

西安交通大学出版社

内 容 简 介

本书全面介绍了加密解密的起源、发展和最新成果，系统地、详细地介绍了二十几种加密技术，给出了实现的方法和参考程序，介绍了解密的工具和解密的思想及方法。此外，还介绍了反跟踪的技巧和实现方法，书中同时给出了构造加密系统的思想和方法，在最后一章给出了加解密实例。本书既包含了目前国内外流行的各种加密技术，又有作者自己独特的创新。书中给出的程序对从事计算机应用的技术人员有很大的参考价值。

(陕)新登字 007 号

磁盘加密解密实用技术

林宝雄 主编

谭晓生 王卫东

责任编辑 伍瑾

*

西安交通大学出版社出版

邮政编码 710049

西安交通大学出版社印刷厂印装

陕西省新华书店经销

*

开本 787×1092 1/16 印张 23.625 字数：574 千字

1992 年 6 月第 1 版 1992 年 6 月第 1 次印刷

印数：1——10000

ISBN7-5605-0476-0/TP・49 定价：12.00 元

前 言

随着软件的商品化，磁盘加密显得愈来愈重要。磁盘加密能有效地保护软件开发者的利益，阻止非法拷贝，这项技术受到软件开发者的高度重视，得到了迅速的发展，与此同时，磁盘解密也相得益彰，发展迅速。磁盘加密与解密的关系是矛与盾的关系，它们相互促进，共同发展。加密的目的是为了保护软件开发者的利益，是受法律保护的；解密则相反，它是要无偿地享受他人的劳动成果，是受非议的，但是作为一种客观存在，人们不得不去研究它，只有充分了解解密的各种技术和方法，才能进行更完善更有效的加密。

磁盘加解密技术源于又别于通信中的加解密技术，因而它既承袭了通信中加解密的方法，又具有自己的特点，经过人们的不断探索，归纳总结出了一系列行之有效的方法。本书共分九章，全面地介绍了目前世界上流行的各种加解密技术和方法，介绍了加密思想的保护技术——反跟踪技术，讨论了加解密中存在的问题，给出了解决的办法。此外，书中还对加解密所需的基础知识作了介绍，这些知识不但对于从事加解密研究的人员是必需的，而且对于计算机工作者和计算机用户也是非常有益的。本书的第一、二、五、九章及附录部分由林宜雄同志编写，第三、六章由王卫东同志编写，第七、八章由谭晓生同志编写，第四章由三人共同编写。

冯博琴副教授仔细审阅了全稿，提出了许多宝贵的修改意见，在此表示衷心的感谢。这里还要感谢众多的编辑们，她（他）们为本书的出版付出了辛勤的汗水，没有她（他）们的辛勤劳动，本书不可能这么快就与读者见面。

由于时间仓促，加之作者水平有限，书中难免有许多错误和遗漏之处，敬请广大读者不吝指教。

作者

1991.11

目 录

第一章　磁盘加解密技术概述

计算机发展到今天，磁盘已经成为计算机中最主要的外部存储器。由于磁盘的大容量和存储信息的安全性，人们乐于用磁盘来保存程序和数据。磁盘已经成为各种软件的传播媒介，全世界流行的各种软件几乎都是通过磁盘的传递来达到共享的。如果忽略计算机网络，可以说没有磁盘就没有软件的共享，没有磁盘就没有信息的共享。目前，磁盘正向大容量和高密度的方向发展。

磁盘是信息的载体也是信息传递的媒介。磁盘上的信息是由程序和数据构成的，因而磁盘上的信息是有价的，有价的东西是需要购买的。由于磁盘的可复制性和可互换性，磁盘上有价的信息就得不到保护，因而从磁盘的诞生之日起，就提出了磁盘的加密问题。磁盘的加密就是既要利用磁盘来传递信息，又要保证信息生成者的经济利益，这个问题的求解就演化成了今天的磁盘加密技术。

磁盘的解密技术与磁盘的加密技术相生相长，从哲学角度来讲，它们是矛与盾的关系；从法律角度讲，加密技术是为了保护软件开发者的经济利益，是一门受法律保护的技术，而解密技术则相反，它是要"无偿"地享用他人的劳动成果，是一门受非议的技术，但是作为一种客观存在，解密技术的发展丝毫不逊色于加密技术，它们互相影响，共同向前发展。加密技术的每一新的发展，都导致解密技术新的突破，而解密技术的每一新的突破又导致加密技术的新发展，它们间的相争相克永远是一个没有结局的矛与盾的"竞技"。

在国外，磁盘加解密技术的研究风起云涌，各计算机研究机构和计算机公司，特别是计算机软件公司十分重视这项技术，他们投入巨大人力和资金进行研究，取得了一系列研究成果和应用成果，最著名的是美国的获专利的激光加密技术。他们不遗余力这样做的目的是为了保护他们自身的经济利益。在美国，虽然制订了软件保护法规，但是单有法规而没有相应的技术保证，法规就只能是法规。在国内，迄今为止软件尚未形成一个产业，软件开发者的利益得不到有效的保障，可以说，国内软件的保护基本上是靠加密技术来保证的。这在客观上刺激了我国加解密技术的发展，导致了各种加解密系统的问世。

磁盘加解密技术是一项特殊的技术，通常一项新的加密技术总是被研究者严守着秘密，计算机方面的各种刊物上很少有其实质性的研究报告。这种新的技术只有假以时日，在一段时间后通过解密者的解密才能被人们所了解和掌握。这从另一侧面佐证了解密技术对于加密技术发展的重要推进作用。从这个意义上讲，解密技术又是功不可没的。

磁盘的加密不能一劳永逸，磁盘无论如何加密都终将被破解，那么磁盘加密是否有意义呢？回答是肯定的。因为任何软件都是有生命周期的，在生命周期内软件能得到有效保护即达到了预期的目的。这就是为什么加密系统推陈出新、层出不穷的原因。

磁盘加密不是一个科学的术语，而是一个通俗的叫法。从科学性、合理性的角度讲，"磁盘加密"应该改为"磁盘反拷贝"，"磁盘加密技术"应该称为"磁盘反拷贝技术"。通俗性即是社会

性，为了不悖于广大读者的旧有心理，本书沿袭通俗的叫法。

磁盘加解密技术是一项研究磁盘拷贝和反拷贝的技术，它不是一个单一的技术，与它相关的，有跟踪和反跟踪技术以及密文和反密文技术，此外还有一些辅助性的技术，这些将在本书的其余章节里详细讨论。

第一节　磁盘加解密的起源

人们最初研制计算机的目的是用于科学计算，解决科学计算中复杂而繁重的人工劳动，但是计算机的发展远远超出了人们最初的想象。今天的计算机已广泛用于过程控制、信息处理和人工智能等领域，计算机已深入到人们生活的各个角落。

计算机的广泛使用自然而然地提出了计算机通信问题，通信是连接计算和处理的唯一途径。计算机通信从大的方面讲，可分为机内通信和机间通信。机间通信一般要穿越人们所不能控制的空间，这就出现了信息"泄漏"和"盗用"问题，而机内通信则一般不存在这个问题。电子辐射是信息泄漏的主要原因，盗用则存在着明显的政治、军事和经济的目的。防信息泄漏和盗用产生了计算机通信中的加解密技术。

信息泄漏和盗用是一种不由人们的主观意志所能控制的客观存在，那么如何防止信息的泄漏和盗用呢？计算机通信中的加解密处理解决了这一问题。

信息的原来形式称之为明文，明文经过加密处理就变成了密文。密文和明文在内容上大相径庭，但密文与明文存在着一种唯一的对应关系，这种关系就是解密算法。解密算法和密钥的结合才能把密文转换成明文。解密算法是可破解的，但了解了解密算法而没有密钥同样无法获得明文，因而经过加密处理的信息即使泄漏和被盗用，被他人获取的也仅仅是一堆无用的信息"垃圾"，从而保证了信息的机密性。通常，密钥和密文不是一起传送的，密钥可以预先或延后通过别的途径传送，交给认可的目标。

明文和密文之间的转化产生了密码技术，从传统密码技术到现代密码技术，形成了一个独立的研究分支——密码学，这些内容不是本书的重点，将在第六章中加以简单介绍。

计算机通信中的加解密可以达到信息保密的目的，那么磁盘中的程序能否加以保护而只传递给认可的目标呢？这个启示和联想形成了最初的磁盘加密的雏形。事实上，磁盘的加解密正是源于通信中的加解密，通信加解密中的思想、方法和技术完全可以被借鉴或使用来实现磁盘的加解密，磁盘中的一些加解密技术、方法和思想直接取自于通信中的加解密技术、方法和思想。

磁盘加解密技术与通信中的加解密技术既有相似之处，又有很大的差异。通信中被加密的对象通常是一种数据，或者至少被当作数据来处理，而不是一般在计算机上能运行的程序；磁盘中被加密的对象则是能被运行的程序。解密算法和密钥共存，因而源于通信中加解密的磁盘加解密又派生出了自己独有的技术。这些内容将在下面章节中详细介绍和讨论。

追踪磁盘加解密技术产生、发展的历史渊源，使我们认识到磁盘加解密与通信中的加解密密切相关，通信中加解密的研究成果可以应用到磁盘加解密中。

第二节　磁盘的可加密性与可破解性

1. 磁盘的可加密性

对磁盘进行加密，其目的是为了防止磁盘的任意拷贝。然而磁盘上的信息是可复制的，即磁盘是可拷贝的，这是一个矛盾，它约束了磁盘的加密，困惑了许多加密研究者，似乎不可解。

磁盘是存储信息的介质，其上的信息可被任意次复制，因而对于程序来说，原盘和复制盘是很难区分的。但是如果从另一角度思考问题，就会找到问题求解的思路。

磁盘的可复制性归结为这样一个问题来认识，即磁盘的无特殊性或一般性，无特殊性是磁盘互换性的原因。那么可否给磁盘附加特殊的标记使其具有特殊性呢？循着这个思路，演生出了为磁盘作特殊标记的许多方法，如在磁盘上产生激光点、在磁盘上穿孔等等，要说明的是这些标记应该是不可复制的，否则就没有意义了。

磁盘有不可复制的特殊标记，给识别原盘还是复制盘提供了可能，这种给磁盘附加特殊标记的方法的可行性，从一个方面证实了磁盘的可加密性。

磁盘无特殊性是基于人们一般认识而得出的结论，事实上，被机械电子式的磁盘机规划出来的磁盘，本身就存在着可以辨识的特殊标记，只是人们在日常的磁盘操作中，对存在于其本身的标记没有去"透视"或关心罢了。这种有意识的"透视"产生了磁盘"指纹"制作和识别技术。这种存在于磁盘本身的"指纹"的可制作和可识别，从又一个方面证明了磁盘的可加密性。

至此可以得出结论，磁盘不但可以加密，而且有众多的加密方法。正是基于这个理由，目前世界上有众多的计算机工作者从事磁盘加密研究工作。

2. 加密磁盘的可破解性

在人类发展史上，有许许多多千古难解之谜，谜之所以千古难解是因为失却了太多的可求解的线索。那么加密的磁盘是否永远不可解，其谜底只有加密者知道或者加密者也不知道呢？这是从事加密和解密的人都关心的问题。

在对这个问题进行理论分析之前，先看看现实的情况。研究磁盘加密的人成千上万，推出的加密系统难以计数，假如其中有一个系统被理论或者实践证明是不可破解的，那么其它的研究者是否都要失业了呢？

正如前面所提到的，磁盘加密是一种特殊形式的加密，解密算法和密钥共存是磁盘加密的特殊所在。被加密的程序是通过密钥获取、密钥鉴别和解密算法完成原盘识别和正常运行的。从理论上看，密钥和解密算法的共存满足了解密的充要条件，因而从理论上可以证明加密磁盘是可解的，这里仅存在解密难易和解密时间长短问题。

加密磁盘的可解性和实际的解密操作是一个问题的两个方面，一方面理论上可解，另一方面实际的解密操作受加密强度和解密者智力与技术的制约。理论的可解性不等于实际的可解性，它们之间存在着差异，这个差异在其它研究领域也同样存在，这是加密研究者研究兴趣经久不衰的实质的原因。

第三节　磁盘加解密技术的最新发展

磁盘加密技术分为三个方面，即反拷贝技术、反跟踪技术和密文技术。对于一个好的加密

系统，这三个技术都需要恰当运用。磁盘解密技术由磁道分析技术、扇区分析技术和密文分析技术（被加密程序分析技术）构成。早期的磁盘加密技术，主要体现在反拷贝技术上，当时人们主要是研究如何制作不可复制的磁盘特殊标记，这些研究成果较多的是应用在苹果机支持的磁盘上，今天许多微机磁盘加密技术就是源于苹果机磁盘加密技术。早期，微机不如今天这样普及，人们关于计算机的知识也远不如今天这样丰富，有关磁盘操作系统（DOS）、磁盘和磁盘机结构及 DOS 文件系统的认识远不如今天这样深入，因而当时的磁盘加密技术在当时的背景下还是很奏效的，但是当 IBM 微机异军突起，再加上其它微机制造公司的不断出现，微机走进了社会生活的各个角落，与之相应的，有关微机组成原理、微机体系结构、微机外部设备、微机语言的书籍像潮水般涌来，形成了人类发展史上特有的现象——计算机文化，与此同时，计算机软件也变成了商品，并在全球流通。这使得磁盘加密技术必须与其同步发展，原先的技术在保护软件研制者的权益上已显得无能为力。磁盘加密中的反跟踪技术和密文技术在微机迅猛发展的时空中得到了长足的发展。

反跟踪技术和密文技术之所以重要，是因为它们是对加密思想或方法的加密，反跟踪技术、密文技术和反拷贝技术的结合，大大提高了磁盘加密强度，增加了加密磁盘的破解难度。

反跟踪技术主要针对调试软件如 DEBUG，CODEVIEW 等，这些调试软件可以跟踪可执行文件的执行，使人们了解可执行文件执行的每一步。因为任何加密软件在 CPU 实际执行它们的时候都必须是明文，因而通过借助调试软件来跟踪被加密程序的运行，就可以了解加密的思路并最终实现解密。跟踪是解密的前提，反跟踪技术就是研究如何阻止和破坏跟踪的技术。

反跟踪技术的研究产生了一系列行之有效的反跟踪方法和措施。概括起来，可以归结为两类，即直接破坏跟踪法和不相容法。前者主要是破坏或利用跟踪机制来实现被加密程序的反跟踪；后者则是使被加密程序和调试程序不能在内存共存，即被加密程序在一般 DOS 环境下可以正常运行，但在调试程序环境下不能运行或不能正常运行。

反跟踪技术的最新发展，出现了动态反跟踪技术和逆指令流技术，这两项技术是前面介绍的两类反跟踪技术的综合运用，目前在具体实现上还不成熟。但可以相信，这两项技术是非常有前途的。

密文技术的发展比反跟踪技术和反拷贝技术要充分得多，因为它直接来自通信中的密文技术。换位法、替代法和乘积密码是密文技术研究中的最早成果。密文技术的最新发展，形成了现代密码技术，DES 算法、RSA 算法和陷门背包算法是现代密码学中研究的重要内容。

同时，反拷贝技术也在向前发展。反拷贝技术实际上就是给磁盘做特殊标记的技术。这种磁盘标记可分为两类，一类是暂时或很长一段时间内不可复制的标记；另一类是永远不可复制的标记。美国的激光加密技术所作的激光孔属于前者，加密卡、针孔等也属于前者；最新发展起来的高级“指纹”技术则属于后者。对于第一类标记，只要技术发展到可以复制，那么密也就不解自破，而不必进行实际的软件解密操作；对于第二类标记，只有进行实际的软件解密操作，才有可能最终解密，因而与反拷贝技术相应的反跟踪技术和密文技术才显得更有用和更有效。

解密技术的最新发展，主要集中体现在更强和更有目的的跟踪上，与以前利用调试软件进行跟踪不同，新的跟踪方法是利用 DOS，而不是利用调试软件。新的跟踪技术可以设置跟踪参数，通过设置这些跟踪参数，可以获得所需的跟踪结果。要说明的是，对于这种跟踪，被加密程序很难觉察。

第二章　加解密的必备知识

磁盘加解密是一门综合技术。从事磁盘加解密的研究必须具有磁盘结构、磁盘机、磁盘 I/O、汇编语言、DOS 及 DOS 文件系统等方面的知识。

第一节　磁盘的结构

1. 磁盘的种类和规格

(1)分类

目前在微型机上使用的磁盘种类繁多，一般可分为硬磁盘和软磁盘两大类。硬盘采用 Winchester 技术，使用最普遍的是 IBM-3340 型硬盘或与其兼容的硬盘，不同硬盘的差别主要在容量上，而容量是由磁头数、磁道数和每磁道扇区数三因素决定的。软磁盘主要有两类，一类是 13.34cm(5.25 英寸)软磁盘，另一类是 8.89cm(3.5 英寸)软磁盘，这两类软磁盘都有倍密和高密两种。13.34cm(5.25 英寸)软磁盘在国内使用最为普遍，8.89cm(3.5 英寸)软磁盘在欧美使用最为普遍。由于 8.89cm(3.5 英寸)软磁盘保存信息的安全性，因而在我国也已开始流行。

磁盘的分类可表示如下：

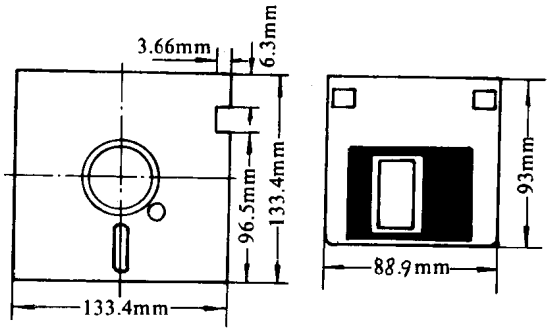
- 磁盘
  - 硬磁盘
    - IBM-3340 型或兼容型
      - 4 磁头，17 扇区 / 道
      - 6/8 磁头，33 扇区 / 道
      - 6/8 磁头，38 扇区 / 道
      - 15 磁头，63 扇区 / 道
    - 非 IBM-3340 型
  - 软磁盘
    - 8.89cm(3.5 英寸) 软磁盘
      - 高密盘(1.44M)
      - 倍密盘(720K)
    - 13.34cm(5.25 英寸) 软磁盘
      - 高密盘(1.2M)
      - 倍密盘(360K)

(2)规格

软磁盘的外形为矩形，其外形尺寸如图 2-1 所示。

硬磁盘盘组的外形尺寸一般是一个 13.34cm 或 8.89cm(5.25 或 3.5 英寸)的正方体，通常密封在一个金属盒内。

表 2-1 列出了磁盘的特征参数。由于硬盘没有互换性要求，因而硬盘的种类很多，表中仅列出常见的几种。这里没有填写磁道数和容量两栏的内容，因为具有相同磁头数和每道扇区数的硬盘其磁道数可能不等，因而其容量也就不等。



(a)133.4mm(5.25英寸)软磁盘　(b)88.9mm(3.5英寸)软磁盘

图 2-1　软磁盘的外形尺寸

表 2-1　磁盘的特征参数

类　型		介质描述符	扇区数/磁道	磁道数	磁头数	容量
13.34cm (5.25英寸)软盘	倍　密	FD	9	40	2	360K
	高　密	F9	15	80	2	1.2M
8.89cm (3.5英寸)软盘	倍　密	F9	9	80	2	720K
	高密	F0	18	80	2	1.44M
硬盘		F8	17 33 38 63		4 6/8 6/8 15	

2. 磁盘的物理结构

磁盘的外形为矩形，其内部实际上是一个个同心圆，这些同心圆构成磁盘的一个个磁道，而磁道又是由一定数量的扇区构成的，各个磁道上的扇区数相等。磁盘的种类虽然繁多，但其物理结构基本相同，所不同的只是盘片数和每道扇区数。磁盘的物理结构如图 2-2 所示。

3. 磁盘的逻辑结构

磁盘上的扇区是用来存放信息的。从这个意义上讲，磁盘上所有扇区的地位是相同的；但是磁盘上的信息是有组织和有序的，因而磁盘上的扇区的作用又是不同的。为了便于管理和存取磁盘上信息，磁盘被划分成 n 个不同的区域，每个区域由相连的扇区构成一个连续的空间。磁盘的这种划分实际上是一种逻辑划分，由此形成的格局就是磁盘的逻辑结构。

图 2-3 和图 2-4 分别示出了软盘和硬盘的逻辑结构，其数据区中包含了子目录区。

4. 磁盘空间的逻辑分布

磁盘的存取是分级的，不同的级存取磁盘的格式不同。下面列出了磁盘存取的三个级：

①DOS 级。调用 INT21H，通过目录、记录的“分块”和“解块”方法访问磁盘，存取的单位是簇；

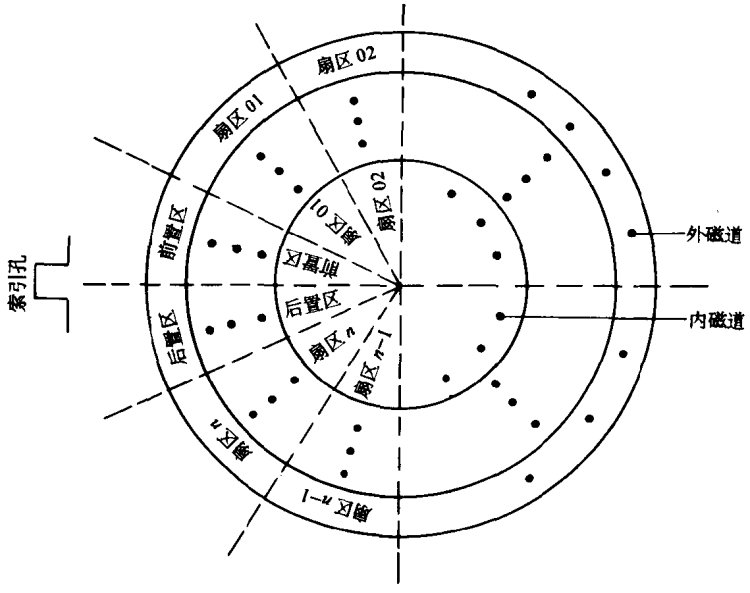


图 2-2 磁盘的物理结构*

*硬盘没有后置区。

②逻辑扇区级。调用 INT25H 和 INT26H，读写时要给出起始的逻辑扇区号和扇区数；

③ BIO 级。调用 INT13H，要以磁头号、磁道号、扇区号和扇区数的形式给出读写磁盘的入口参数。

由于磁盘的分级存取，于是有了磁盘空间的逻辑分布。簇分布和逻辑扇区分布，是目前采用的两种磁盘空间逻辑分布。

(1)软盘空间的逻辑分布

双面双密软盘是应用

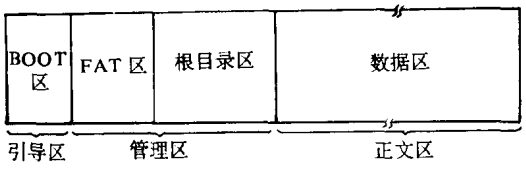


图 2-3 软盘的逻辑结构

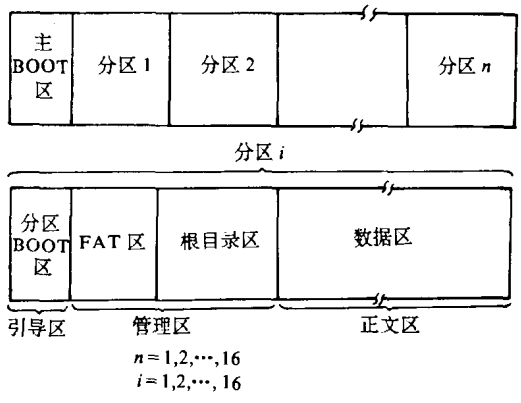


图 2-4 硬盘的逻辑结构

最为普遍的一种软盘，下面即以它为例来描述软盘空间的逻辑分布。其它软盘如单面盘和高密盘具有类似的逻辑分布。

软盘有两个面，两个磁头(磁头 0 和磁头 1)分别对应这两个面(0 面和 1 面)。磁盘上的一个同心圆构成一个磁道，由外向里一共有 40 个同心圆，因此软盘共有 40 个磁道。每个磁道上分布着 9 个扇区，每个扇区都是一个含有 512 个字节的区域。

为了减少磁头寻道时间，软盘的空间是这样编排的：从某一道的 0 面的第一个扇区开始一直排列到这一道的 1 面的第 9 个扇区为止，而不是把一个面上的所有道排完再开始排另一面的所有道。图 2-5 是双面双密软盘的簇分布图。

0 面

	1	2	3	4	5	6	7	8	9
磁道 0	BOOT	FAT1		FAT2		ROOT			
磁道 1	5.1	5.2	6.1	6.2	7.1	7.2	8.1	8.2	9.1
磁道 2	14.1	14.2	15.1	15.2	16.1	16.2	17.1	17.2	18.1
· · ·									
磁道 39	347.1	347.2	348.1	348.2	349.1	349.2	350.1	350.2	351.1

1 面

	1	2	3	4	5	6	7	8	9
磁道 0	ROOT			2.1	2.2	3.1	3.2	4.1	4.2
磁道 1	9.2	10.1	10.2	11.1	11.2	12.1	12.2	13.1	13.2
磁道 2	18.2	19.1	19.2	20.1	20.2	21.1	21.2	22.1	22.2
· · ·									
磁道 39	351.2	352.1	352.2	353.1	353.2	354.1	354.2	355.1	355.2

图 2-5　双面双密软盘的簇分布

从图中可以看出，软盘没有第 1 簇，是从第 2 簇开始排列的，这主要是为了在 DOS 中方便对簇的访问和管理。

推断 i 道 0 面 1 扇区簇号的公式为

$$(i-1)\times 9+5, i=1,2,\cdots,39$$

由上式可以把所有道上的扇区的对应簇号填写出来，以备实际使用时查找。

从图 2-5 中可知，0 道 0 面 1 扇区是引导记录所在扇区即引导扇区，0 道 0 面 2—3 扇区是第一文件分配表 FAT1，4—5 扇区是第二文件分配表 FAT2，0 道 0 面的 6—9 扇区以及 0 道 1 面的 1—3 扇区共 7 个扇区是根目录(ROOT)区。从第二簇开始是 DOS 的文件区。

图 2-6 是双面双密软盘的逻辑扇区分布图。

0 面

	1	2	3	4	5	6	7	8	9
磁道 0	0	1	2	3	4	5	6	7	8
磁道 1	12	13	14	15	16	17	18	19	1A
磁道 2	24	25	26	27	28	29	2A	2B	2C
· · ·									
磁道 39	2BE	2BF	2C0	2C1	2C2	2C3	2C4	2C5	2C6