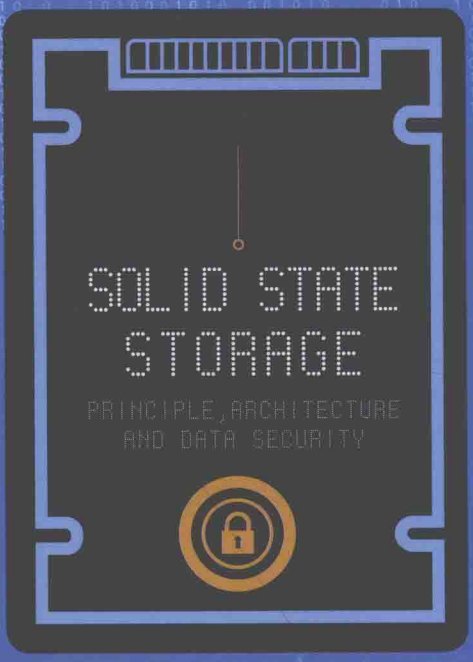


固态存储

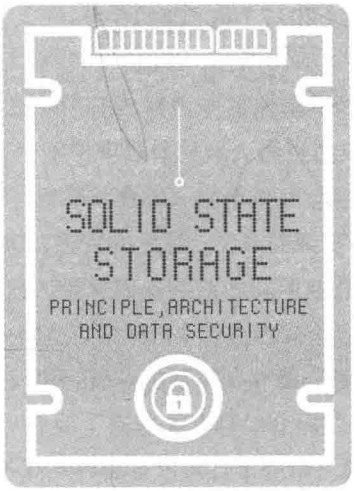
原理、架构与数据安全

夏鲁宁　贾世杰　陈波　◎著

固态存储突破现有存储性能瓶颈

本书详解固态存储的原理及架构设计，重点阐述数据存储的安全技术、存储数据机密性保护

机械工业出版社
China Machine Press



固态存储

原理、架构与数据安全

夏鲁宁　贾世杰　陈波　◎著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

固态存储：原理、架构与数据安全 / 夏鲁宁，贾世杰，陈波著 . —北京：机械工业出版社，2017.8

ISBN 978-7-111-58001-0

I. 固… II. ①夏… ②贾… ③陈… III. 存储器 IV. TP333

中国版本图书馆 CIP 数据核字（2017）第 222215 号

固态存储：原理、架构与数据安全

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码：100037）

责任编辑：余 洁　　责任校对：李秋荣

印　　刷：北京文昌阁彩色印刷有限责任公司　　版　　次：2017 年 9 月第 1 版第 1 次印刷

开　　本：186mm × 240mm 1/16　　印　　张：21.25

书　　号：ISBN 978-7-111-58001-0　　定　　价：69.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

客服热线：（010）88379426 88361066　　投稿热线：（010）88379604

购书热线：（010）68326294 88379649 68995259　　读者信箱：hzit@hzbook.com

Preface 前　言

不同于磁带、机械硬盘、光盘等依托机械运动实现读写的存储技术，固态存储器（solid-state memory，简称固态存储）完全基于半导体技术，通过改变芯片内部固态存储介质的状态（比如电荷、相变、极化和电阻等）来存储数据。在传统磁盘存储系统性能停滞不前的情况下，固态存储以崭新的视角，经过多年的研究和发展，为存储领域带来了一场革命性变革，成为突破现有存储性能瓶颈的希望。然而，随着固态存储的应用和普及，数据存储安全性、机密性、可靠性等问题逐渐凸显。如何解决固态存储架构中存在的安全问题将是本书中的浓墨重彩之处。

全书共 11 章，可分为三部分：第一部分包括第 1~3 章，介绍存储技术的基础知识。第 1 章简要回顾了存储技术的发展历史，介绍了当前主流存储介质的工作原理和特点，随后对磁盘阵列、网络化存储和大数据时代下的新兴存储技术进行了介绍，最后简介了存储系统的逻辑构成。第 2 章对当前主要文件系统，如 FAT、EXT、NTFS、CDFS，从基本概念、存储结构、存储特点等方面作了详细的阐述并进行了对比，随后对其他一些文件系统，如 BtrFS、ZFS、HFS 等进行了简单介绍。第 3 章讲述存储系统的接口与协议，简单阐述了接口与协议的基本概念，详细介绍了计算机系统中常用的存储器物理协议和接口，并对各个接口和协议的发展、特点以及原理进行了详细的分析。

第二部分包括第 4~7 章，介绍了固态存储的原理与架构。第 4 章对固态存储技术进行了概述，详细介绍了基于 NAND Flash 和 NOR Flash 的固态存储原理。第 5 章以日常工作、生活中广泛使用的固态硬盘（SSD）为例给出了固态存储架构，并详细介绍了固态存储系统各大基本部件的结构、功能和原理。第 6 章主要针对固态存储设备中广泛使用的嵌入式文件系统，如 JFFS、YAFFS、UBIFS 以及 exFAT 等文件系统，从内存结构、文件系统挂载、运行原理、垃圾回收等方面，详细介绍固态存储文件系统的原理和运行机制。第 7 章主要对固态存储设备中的容错与平衡技术进行了介绍，首先介绍了三种纠错码即汉明码、BCH 码以及里德 - 所罗门码的操作原理，接着介绍了固态存储的平衡机制，分别从垃圾回收和使用均衡两个方面介绍其作用和实现原理，最后介绍了固态存储器件的坏块管理与实现。

第三部分包括第 8~11 章，介绍了固态存储安全技术及对前沿科技的展望。第 8 章详细介绍了为提高固态存储设备的数据安全，学术界提出的各种技术方案。第 9 章首先讨论固态存储设备中数据加密的主要算法 XTS-AES，随后简单介绍了近年来学术界提出的多种可否认加密与可

否认认证协议方案，然后根据面向系统平台的不同，着重介绍可否认加密技术在数据存储方面，尤其是固态存储设备上的各种应用方案。第 10 章介绍了为保护存储设备数据安全，学术界提出的基于 NAND Flash 物理特性，提取设备指纹、随机数、密钥等信息及其应用实例。第 11 章对存储技术的发展作了展望。

前 3 章内容较为基础，第 4~7 章为固态存储相关基础知识，第 8~10 章则为固态存储领域以及作者自身团队与安全相关的研究成果，内容较新，最后一章为展望，读者可根据自己的兴趣和时间情况选择阅读。

固态存储发展极为迅速，目前已成为一个新兴热点领域。云计算、物联网、大数据时代的到来，为存储技术的创新带来了新的机遇和挑战。随着新型固态存储介质的日渐成熟，延时越来越低，带宽越来越高，以动态随机存储器为代表的易失型存储设备在主存中的垄断地位将可能被非易失型固态存储设备所取代。而不断增大的容量和不断降低的价格，使固态存储技术越来越适合于构建高性能的外部存储设备。以磁盘为代表的机械驱动外部存储设备的主流地位将逐步被固态存储设备取代，使得存储系统的访问模式可能转为利用电子设备的电气特性而非机械转动。总之，固态存储已成为数据存储发展的必然趋势，其安全性、机密性、可靠性等值得关注。

本书的研究工作得到国家重点基础研究发展计划（973 计划）2013CB338001 课题的支持。在本书的编写和出版过程中，得到了机械工业出版社的大力支持，在此谨表诚挚的谢意。

由于作者水平有限，加之固态存储技术发展迅速，书中不妥和错误之处在所难免，诚恳地希望专家和读者提出宝贵意见，以帮助本书改进和完善。

Contents 目　录

第一部分 Part 1

存储技术基础

信息技术的日新月异使社会对信息存储的需求逐日攀升，同时借力于大数据分析，信息存储为社会带来的价值也日益增大。作为信息管理的基石，信息存储技术已经发展成为一门既复杂又成熟的分支学科，它需要满足信息管理的高性能、可扩展、可共享、高可用、自适应和可管理等一系列需求，是一门非常关键的技术。

数据存储是人们一直以来都在应用并且探索的主题。在原始社会，人们用树枝和石头来记录数据。后来，人们用铁器在石头上刻画一些象形文字来记录数据，但此时记录的内容也只有自己能看得懂。再后来，随着语言、文字、造纸、印刷等技术的出现，信息得到了更加长久地存储。而随着科学技术的发展，纸带、软盘、硬盘、光盘等成为主要的存储介质。

本书第一部分描述了与存储技术有关的基础知识，包括第1~3章的内容。

第1章介绍了存储技术的基本概念，回顾了信息存储技术的发展历程，简单介绍了目前主流的物理存储介质，如磁介质、光介质以及半导体存储器，并分析其基本组成和工作原理，以及各自的特点，并对磁盘阵列技术进行了介绍。同时也介绍了当前主流的网络存储技术和分布式存储技术的相关概念、原理、特点等内容，论述了其基本体系和组成。最后对存储系统的基本组成作了简单介绍。

第2章介绍了一些主要的文件系统，包括FAT、EXT、NTFS、CDFS，并从不同文件系统的发展概况、基本概念、存储结构、存储特点等方面作出详细的阐述。此外，还简要介绍了其他一些文件系统，如BtrFS、ZFS、HFS、HFS+、ReiserFS、JFS、XFS、UFS、VMFS、VxFS、ReFS等，并分析其各自的特点。最后对常用的文件系统进行了对比，讨论它们之间的区别和各自的优缺点。

第3章介绍了存储系统的接口与协议，简单阐述了接口与协议的基本概念，详细介绍了计算机系统中常用的存储器物理协议和接口，包括IDE协议及接口、SCSI协议及接口、FC协议及接口、SATA协议及接口、SAS协议及接口、PCI-E协议及接口、eMMC协议及接口，并对各个接口和协议的发展、特点以及原理都进行了详细的分析。

第 1 章 Chapter 1

存储技术概要

存储器作为电子产品的数据存储支撑，在整个产业中占有核心地位。近几十年来，新的存储技术不断涌现，推动了存储设备的快速更新换代。在 20 世纪 50 年代，由于体积庞大，存储器仅能运用于大型计算机，如今的存储器早已今非昔比，其体积小、性能高、容量大，可运用于各个领域，成为开启大数据时代的基石。本章首先回顾了存储技术的发展历史，随后介绍了当前的主流存储技术及大数据时代下出现的新型存储技术，最后介绍了存储系统的逻辑构成。

1.1 存储技术发展简史

信息存储是自古就有的话题。特别是数字化信息技术诞生以来，关于数字信息存储的技术不断演进和发展，并持续得到学术界和工业界的关注。

信息本身是没有物理形态的，只有经过载体的承载才能进行存储、传递和共享。长期以来，人们都在不断探索保存信息的方法和载体。起初人们借助于不同颜色的石头、在绳上打结等方式来记事，这是信息存储的早期方式。随着语言、文字的出现，信息存储技术迎来了一次质的飞跃，人们可以将信息记载到一些载体上，使得信息能够长期有效地保存。尤其是造纸术的发明，它结束了人们利用石头、竹简、金属、兽骨等高成本、低密度载体的历史，而印刷术的出现则终结了以手抄和篆刻文献为主的时代，使得信息能够大量记录并长久保存，大大增强了人类知识积累的能力。

随着科学技术的不断发展，社会信息量急剧增加，信息的飞速增长是当今社会一大特点。由于纸张存储存在体积大、不利于查阅和维护等问题，用纸张存储信息的局限性便逐渐暴露出来。计算机技术的出现和发展很好地解决了这些问题，而计算机技术与现代通信技术

的结合使信息处理速度和存储效率得到了惊人的提高，人类处理信息的能力也得到了很大的发展。因此，现代信息存储技术的发展与计算机的发展密不可分。

目前，主流的信息存储手段主要是利用磁介质、光介质或半导体介质等相关技术实现。早期的计算机系统没有磁盘，利用在纸带上打孔来进行数据存储并作为输入计算机系统的手段。发明磁存储技术之后，磁带是主要的数据存储介质，相对纸片打孔而言，磁带的读写速度快了很多，而且易于保存。由于成本低廉，磁带库在目前一些网络存储系统中仍被广泛应用。

进入21世纪以后，网络日益发达，计算机技术也不断进步，信息量更是成倍地增长。为了应对海量数据的存储，工业界持续致力于硬盘容量的提升，然而在有些场合下仍旧无法满足信息存储的需要。在海量存储需求的推动下，将大量磁盘连接起来的磁盘阵列技术被设计出来，以提供更大的存储空间。磁盘阵列一般部署在网络之中，作为专门提供存储服务的网络节点而存在。目前主要的三种网络存储架构是DAS、NAS、SAN。其中，DAS（直连式存储）是一种以服务器为中心的存储架构，服务器直接通过SCSI接口与磁盘阵列连接，服务器端的磁盘阵列端口不能共享，客户端需向服务器发送连接请求，然后获得由服务器转发而来的信息。随着网络技术和光纤技术的发展，DAS逐步被其他方式取代。NAS（网络附加存储）即通过直接连接或外部连接到网络上，使得网内的信息处理设备能够直接对其进行读写。NAS拥有专门的文件和操作系统，实现了文件服务的优化，并且具有异构共享能力，使不同操作系统下的用户可以方便存取任意格式的文件数据。而SAN（存储区域网络）中，服务器采用专用网络实现对磁盘阵列的读写，是一种利用光纤集线器、光纤路由器、光纤交换机等网络互连设备将磁盘阵列和服务器互连起来的面向网络、以数据为中心的存储架构。在SAN模型中，多个服务器能够访问磁盘阵列中的同一个端口。

除了容量，信息的存取速度是随着存储需求的提升而面临的另一个瓶颈。传统硬盘由于机械架构的存在，其响应速度的提高存在限制，而目前硬盘的主轴转速基本没有太大的提高空间了。硬盘的发展显然要落后于其他硬件，并逐渐成为PC中的瓶颈之一，直到固态硬盘的到来才让硬盘真正进入高速发展的时代。固态存储是指以半导体存储器件为介质进行数据存储和读取的一种技术，早期的固态存储技术主要是基于动态随机存储器（Dynamic Random Memory，DRAM），但是由于其断电后存储的数据就会消失，严重制约了其应用范围。近年来基于闪存（Flash Memory）的固态存储技术日趋成熟，并在大容量存储方面发挥着越来越重要的作用。

信息技术的发展不可避免引发对信息安全的关注。在日常工作、生活以及学习中，人们越来越依赖信息技术，越来越多的数据被存储在计算机系统中，存储系统必须保证这些数据的高可用性和高安全性。随着存储系统由本地直连向着网络化和分布式的方向发展，并被网络上的众多计算机共享，存储系统变得更易受到攻击，相对静态的存储系统往往成为攻击者的首选目标。因此，存储安全变得至关重要。既要保证文件数据完整、可靠、不泄密，又要

保证只有合法的用户才能够访问相关的文件，因而存储安全成为信息安全研究领域的焦点话题之一，主要涉及存储加密技术、数据清理技术、数据备份及灾难恢复技术等。

1.2 存储介质

“存储介质”是存储信息的载体。不同的存储介质有不同的物理形态，并采用不同的物理原理来承载信息。例如，纸张就是一种存储介质，文字信息以墨水书写的方式加载到纸张之上。在现代社会的信息化领域，绝大部分信息是以数字形式存在的，因而存储介质主要被用作存储二进制的“0”或“1”。数字信息的存储介质实质上是实现数字信号表示的物质或元器件，这种物质或元器件具有表现两种相反物理状态的能力，这两种物理状态的改变速度决定了存储器的存取速度。存储介质是构成存储设备的基础，目前常用的数字存储介质有磁存储介质（简称磁介质）、光存储介质（简称光介质）和半导体存储器等，下面将以此顺序介绍各种相关的存储技术。

1.2.1 磁介质

磁存储介质利用磁场和磁感效应来产生读写二进制数据的环境，根据其外形可分为磁带、磁鼓、磁盘等。磁带存储容量大、价格低、适合长期保存，可以在较低的成本下实现具有 TB 级存储容量的存储系统。磁盘是各种计算机系统中被广泛使用的大容量外存储器，早期磁盘可分为硬盘和软盘两类。硬盘盘基用非磁性轻金属材料制成，容量大、存取速度快；软盘盘基用挠性塑料制成，容量小、可拆卸、携带方便。

1. 软盘

在 20 世纪 60 年代末 70 年代初期，IBM 公司推出全球第一台 PC，为解决计算机操作指令的存储问题，其于 1967 年推出世界上第一张“软盘”，直径为 32 英寸，开启了软盘的研制之路。1971 年，Alan Shugart 推出一种直径为 8 英寸的表面涂有金属氧化物的塑料质磁盘，这就是标准软盘的“鼻祖”，容量仅为 81KB。8 英寸的软盘虽然从技术原理上已经很接近现代软盘，但缺陷就是体积过大，携带很不方便，于是 5.25 英寸软盘诞生了。为了改进 5.25 英寸软盘易损坏、体积较大等缺点，索尼公司于 1980 年率先推出体积更小、容量更大的 3.5 英寸软驱和软盘，以其便宜的价格、相对更大的存储容量很快全面占领市场。20 世纪 90 年代，3.5 英寸 /1.44MB 软盘一直是 PC 的标准数据传输方式之一。图 1-1 为各种规格的软盘。然而，随着社会信息量的迅速增加，软盘容量过小、读写速度慢、寿命短、可靠性差、数据易丢失等缺点逐渐显露出来，已不能满足数据存储的需求。特别是在以 U 盘为代表的大容量可移动存储器出现之后，软盘渐渐地淡出了人们的视线，时至今日已经少有 PC 支持软盘驱动器。

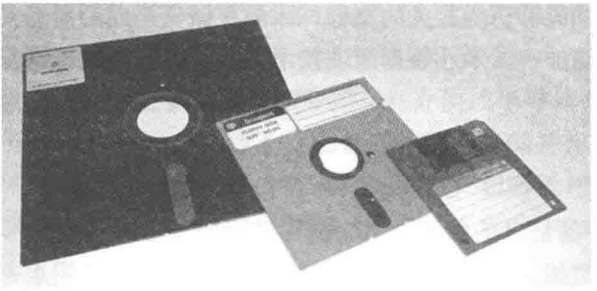


图 1-1 各种规格的软盘

2. 硬盘

1956 年，IBM 公司制造了第一款硬盘驱动器 IBM 350 RAMAC，包含 50 张 24 英寸的盘面，容量不到 5MB，读写速率为 1.1KB/s。以现在的眼光来看待 IBM 公司 350 RAMAC 还算不上真正意义的硬盘，但它开创了信息存储的新时代。随后 IBM 公司于 1980 年制造了 IBM 3380，它是首个容量突破 1GB 的硬盘，总容量 2.52GB，重约 250kg。硬盘自出现之后便成为计算机系统的重要组成部分，与不断改进的计算机外设接口技术相结合，形成大容量、高速率的存储系统。

硬盘自 1956 年诞生以来，跨过了 60 年的风风雨雨，已经成为计算机主要的存储媒介。回顾当年 IBM 公司发明的世界上第一块硬盘仅有 5MB 的存储空间，却由 50 张 24 英寸的碟片组成，所占体积在现今人们对计算机的理解来看是不可想象的。1973 年，IBM 公司又成功研制了新型的曼彻斯特硬盘，拥有两个 30MB 的存储单元，其体积大大缩小，存储密度也大为提高。随后，硬盘驱动器也从控制技术、接口标准、机械结构等方面进行了一系列的改进，硬盘朝着大容量、小体积、高读取速度的方向不断发展。硬盘的尺寸也从最初的 5.25 英寸和 3.5 英寸再降到了 2.5 英寸，其应用领域也从 PC 拓展到了便携式电子产品。固态硬盘的出现是硬盘技术的一个重大变革，随着半导体存储芯片的成本逐渐降低、稳定性逐渐提高，固态存储介质已经在消费类电子产品中相当普及，在 PC 领域也大有取代硬盘的趋势。

硬盘是由固定面板、控制电路板、盘头组件、接口及其他附件等组成，其中盘头组件是构成硬盘的核心，封装在硬盘的净化腔体内，包括浮动磁头组件、磁头驱动机构、盘片及主轴组件、前置读写控制电路，硬盘的内部结构如图 1-2 所示。

浮动磁头组件由读写磁头、传动手臂、传动轴三部分组成。磁头是硬盘技术中最重要和关键的一环，实际上是集成工艺制成的多个磁头的组合，它采用了非接触式头、盘结构，加电后在高速旋转的磁盘表面飞行，飞高间隙只有 0.1 ~ 0.3μum，可以获得极高的数据传输率。现在转速 5400rpm 的硬盘飞高都低于 0.3μm，以利于读取较大的高信噪比信号，提供数据传输存储的可靠性。

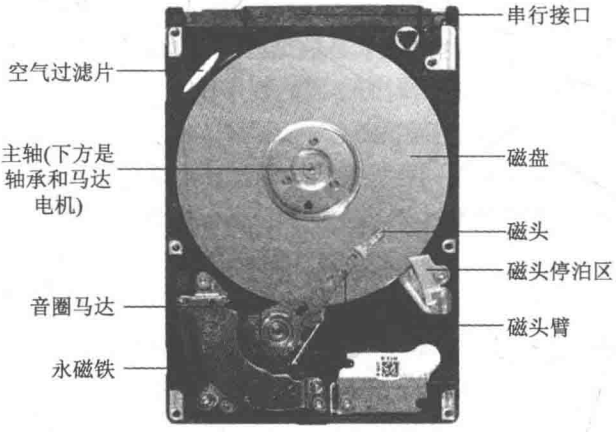


图 1-2 硬盘的内部结构

磁头驱动机构包括电磁线圈电机、驱动小车和防震动装置等。高精度的轻型磁头驱动机构能够对磁头进行正确的驱动和定位，并在很短的时间内精确定位系统指令指定的磁道，保证数据读写的可靠性。

盘片是硬盘存储数据的载体，现在的盘片大都采用金属薄膜磁盘，这种金属薄膜较之软盘的不连续颗粒载体具有更高的记录密度，同时还具有高剩磁和高矫顽力的特点。主轴组件包括主轴部件如轴承和驱动电机等。随着硬盘容量的扩大和速度的提高，主轴电机的速度也在不断提升，有厂商开始采用精密机械工业的液态轴承电机技术。

前置读写控制电路控制磁头感应的信号、主轴电机调速、磁头驱动和伺服定位等，由于磁头读取的信号微弱，将该电路密封在腔体内可减少外来信号的干扰，提高操作指令的准确性。

与软盘类似，硬盘逻辑上被划为磁道、柱面和扇区，其结构关系如图 1-3 所示。

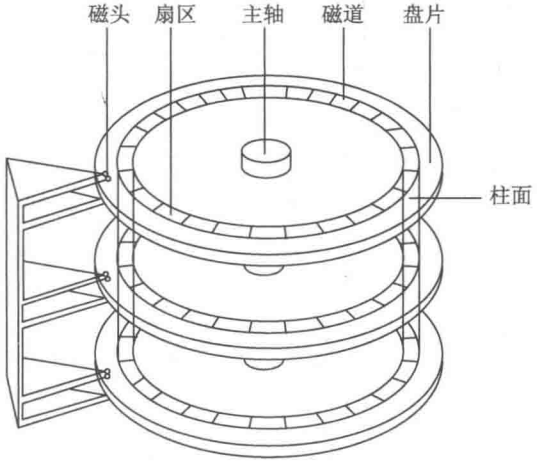


图 1-3 柱面和盘片上的磁道

每个盘片的每个面都有一个读写磁头，磁头起初停在盘片的最内圈，该区域不存放任何数据，称为启停区或着陆区，其他区域就是数据区。在最外圈，0 磁道一般是硬盘数据开始存放的地方，它存放着操作系统启动时所必需的程序代码。所有盘面上同一磁道构成的圆柱即为柱面。每个圆柱上的磁头由上而下从 0 开始编号。磁头读写数据时首先在同一柱面内从 0 磁头开始进行操作，依次向下在同一柱面的不同盘面上进行操作。

硬盘性能好坏是由其相关的技术参数决定的，硬盘的性能参数主要有如下几个：

（1）容量

作为计算机系统的数据存储器，容量是硬盘最主要的参数。硬盘内部往往有多个叠起来的磁盘片，所以说“硬盘容量 = 单碟容量 × 碟片数”。硬盘容量当然是越大越好，以便可以装下更多的数据。要特别说明的是，单碟容量对硬盘的性能也有一定的影响：单碟容量越大，硬盘的密度越高，磁头在相同时间内可以读取到更多的信息，这就意味着读取速度得以提高。

（2）转速

转速是硬盘内电机主轴的旋转速度，也就是硬盘盘片在一分钟内所能完成的最大转数。转速的快慢是标示硬盘档次的重要参数之一，它是决定硬盘内部传输率的关键因素之一，在很大程度上直接影响到硬盘的速度。硬盘的转速越快，硬盘寻找文件的速度也就越快，相对硬盘的传输速度也就得到了提高。

（3）平均访问时间

平均访问时间是指磁头从起始位置到目标磁道位置，并且从目标磁道上找到要读写的数据扇区所需的时间，体现了硬盘的读写速度。

（4）传输速率

硬盘的数据传输率是指硬盘读写数据的速度，单位为兆字节每秒（MB/s），包括内部数据传输率和外部数据传输率，分别反映硬盘缓冲区未用时的性能和系统总线与硬盘缓冲区之间的数据传输率。

（5）缓存

该指标指在硬盘内部的高速存储器。缓存的大小与速度是直接关系到硬盘的传输速度的重要因素，能够大幅度地提高硬盘整体性能。DFT（Drive Fitness Test，驱动器健康检测）程序对硬盘进行检测时，可以让用户方便快捷地检测硬盘的运转状况。

硬盘的容量越来越大，容纳的资料自然也越来越多，这个时候就需要硬盘具有较高的可靠性和安全性，数据保护技术和抗震技术只会变得越来越重要，各个厂商应该在此投入更多的精力。目前主要的硬盘数据保护技术有 S.M.A.R.T 技术、DFT 技术、加密技术等。通过 S.M.A.R.T. 技术，可以对硬盘潜在故障进行有效预测，提高数据的安全性。

1.2.2 光介质

光存储介质的主要代表为光盘存储器，其利用激光读出和写入信息，主要优点是密度