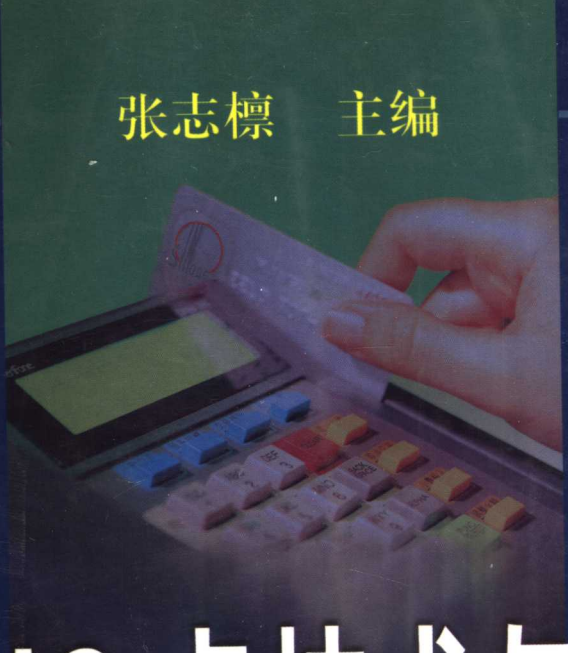
张志檩　主编



加油IC卡技术与应用

中国石化出版社

加油IC卡技术与应用

张志檩　主编

中国石化出版社

图书在版编目(CIP)数据

加油 IC 卡技术与应用/张志檩主编．
—北京:中国石化出版社,2002
ISBN 7-80164-188-4

Ⅰ.加…Ⅱ.张…Ⅲ.智能卡-应用-加油站-销售管理 Ⅳ.U473.8

中国版本图书馆 CIP 数据核字(2002)第 003379 号

中国石化出版社出版发行
地址:北京市东城区安定门外大街 58 号
邮编:100011　电话:(010)84271850
http://www.sinopec-press.com
E-mail:press@sinopec.com.cn
北京精美实华图文制作中心排版
海丰印刷厂印刷
新华书店北京发行所经销
*
787×1092 毫米 16 开本 18.5 印张 467 千字 印 1—3500
2002 年 3 月第 1 版　2002 年 3 月第 1 次印刷
定价:60.00 元

主　　编：张志檩

副 主 编：吴正宏　罗　莉　陈大才　李　勇

编审人员（按姓氏笔画为序）：

王洪伟　王效商　王永祥　王　华　王会丰

韦晓华　孔祥山　李昆明　李　岳　李　勇

吕运春　刘　新　刘芳敏　刘依群　刘　卫

杨江远　杨孝同　吴正宏　张文翔　张春来

张志檩　张经文　张　篷　郑　联　林章春

林　晔　柳征一　罗　莉　周　江　赵世杰

姜　明　姜长中　袁顺昌　韩景林

序

为了总结和交流加油IC卡技术，进一步推进其应用，我们组织业界有经验的公司和工程技术人员编写了《加油IC卡技术与应用》一书。

能源是人类生产、生活的基础，石油又是人类经济活动与生活的“血液”。据统计，1950～1995年间，全球矿物燃料能耗增加了100多倍，其中，美国占75%，年车用燃料达5亿吨。目前，全世界近120个国家拥有近800座炼油厂，原油年加工能力40亿吨以上，年实际加工30多亿吨，每年世界消耗汽、柴油近20亿吨。

环节和链条是哲学范畴中的一对最常见的对立统一体。生产过程、商业流通中皆有之。供应链(supply chain)管理则是解决生产和商业流通领域中产品（商品）供应的对立统一问题。

国外学者和企业家非常重视供应链问题和供应链管理的改善。美国专家估计，供应链各环节的有关费用消耗在产品销售额中占有很大比例，其中在国内销售略小，约占10%，而国际间的贸易则高达40%。因此，提高供应链管理的效率，研究供应链管理的现代模式和技术，则是提高企业竞争力的关键。美国白宫科技政策办公室组织200多名技术专家形成的《美国化学工业2020年技术展望》把改善供应链管理作为美国今后20多年的四大关键技术之一则是最好的例证。正因为如此，该问题也引起了我国经济学家和企业家的重视。但是，我们毕竟起步很晚了。

美国和其他发达国家的连锁商业，可以说是流通领域里流通方式的革命，是计算机和计算机网络的普及，为连锁经营提供了空前的现代化的管理手段。连锁商业从70年代在国外发达国家悄然兴起，到1995年美国零售业销售额为23000亿美元，占GDP的32%，而其56%是由链锁业创造的。其中22%又是由50家最大的零售商所创造。如全球无可争议的最大零售商——沃尔玛则占美国零售业的50%，2000年其营业额达1913亿美元，仅次于埃克森/美孚公司，超过通用和福特公司，居世界500强第二。

沃尔玛从1962年创建，历经30余载，由一家小个体商店发展为全球零售业的巨头。1996年销售额为1061亿美元（1997年近1200亿美元），纯利30亿美元，员工68万名，开设了3054家店铺，其中折扣商店1960家，会员制仓储商店436家，超级中心344家，另外还有20多个配送中心。2000年，员工达120万，拥有4000多家商店。沃尔玛具有超凡的业绩，主要是其重视科技，特别是

信息技术的结果，这是它在激烈的商战中立于不败之地的主要法宝。在沃尔玛总部，建立了庞大的数据中心，全集团的几大分公司，所有店铺、配送中心以及经营的10万种以上的商品，每天所发生的一切与经营相关的购、销、调、存等详细信息，都通过主干网和通信卫星传送到总部中心。中心数据库的最宝贵资源就是信息。信息量正在以天文数字般的飞快速度增长，1991年，数据总量还不到1TB(tera byte,千亿字节),1995年增至5TB，1997年又增至24TB，1998年后超过100TB。他们在从事由数据变信息，由信息变知识的知识挖掘工作。通过全球、全集团、全方位、全过程、全天候的自动数据采集技术，改变传统的依靠假设和推断来确定订货的方式；从数据的不断积累过程中，以小时为单位动态地运行决策模型，导出数亿个品类的最佳订货量，最佳商品组合、分配、降价以及商品最佳陈列等。沃尔玛与生产商、供应商建立了实时链接的信息共享系统，也就是他们称谓的“制造销售同盟”,赢得了比其竞争对手（如凯马特）管理费用低7%，物流费用低30%，存货期由6周降至6小时的优异成绩。

国外的石油、石化公司也非常重视产品销售环节及整个供应链的管理。像重视生产一样，重视销售环节，甚至由销售环节牵动生产环节、研发环节。例如，Amoco公司在1994年即建成了总部与下属的5000多个加油站通过银河7号通信卫星联结的实时信息交换专用网络，方便了油品调配和加油管理。各地加油站的油品销售情况经卫星实时地传到地区储油中心，经过分析处理后再传至总部。总部对市场、资源、成本和最短输油途径等因素综合评价后，向有关炼油厂分配生产额。于是在几个小时内，炼油厂几十套生产装置即可按改变的生产计划满足市场需求。Texaco于1993建成了从总部到商务中心、输油管线监控站（40余处）、炼油厂、储油库、油罐车队（60余个）和2150个加油站的卫星专用网络。Chevron石油公司的卫星专网规模更大，总部和70多处销售中心、60多处储油库、油罐车队及5500多个加油站相联结。日本第三大石油公司Cosmo1986年组建，1987年10月即开通全国综合数字通信网，1988年成立全资Cosmo信息网络公司，从事加油卡自动售油业务的支持，10月，自动售油系统投入运营。短短几年时光，就由网络控制了遍布日本四大州岛的全部炼油厂、销售公司、油库和数千个加油站。实现了网络化和加油自动化。Exxon公司总部设数据中心，美国本土设12个分中心，管理数百个应用系统，沟通市场营销、零售卡运作、顾客投诉以及运输船队。Exxon与Mobil重组后，拥有15000个销售网点，分布在全国43个州，其中9000个为公司直接经营，日销售量达10万吨左右。其中设便利店者达60%左右，设汽车维修保养者达40%左右。加油站的装备包括全自动加油机、现金收款机、刷卡读卡机以及讯号传输器(speadpass),实时报告销售业绩和库存情况。加油机为一机多枪，多种品种加油，多为自助方式，加油口设油气回收装置。零售自动化中磁卡交易占50%，并有油库自动管

理、室内外录像监控，自动化程度很高。Dow Chemical 公司用大型计算机将商业活动和生产工艺变化链接，通过全球化的网络使注意力集中到最佳供应链上。中央数据库即能反映全球订货的实际时间变化。

总之，国外大公司非常注意供应链的管理，注重供应链管理中重要的支柱技术——信息技术。例如，1935 年美国每生产一美元产品，要在信息处理上花去 15 美分。到 1965 年则升至 25 美分，到 1975 年，又升至 36 美分。信息投入越来越大，信息消费越来越多，信息成本也越来越高，同时，也说明信息在当今和未来经济发展中的作用也越来越大。据美国《信息周刊》介绍，1997 年美国应用信息技术最多的 500 家公司平均每家投入 2.3 亿美元，比上年增长 8%。按行业看，投入占营业收入的比重平均达 2.9%，最高达 6.6%。石油化工行业约占 1%～2%。目的是维持先进的基础设施和手段，向电脑空间(syberspace)进军，开拓业务，降低成本，取消非增值环节，提高工作效率和经济效益。

改革开放以来，我国经济得到了突飞猛进的增长，至 1999 年，国内生产总值排世界第七位。至 2000 年，我国综合国力居世界第 9 位。据统计，到 1999 年末，全国设市 667 个，建制镇 16000 多个，100 万以上人口的特大城市 32 个，城镇居民 3.5 亿，预计 2010 年，城镇人口将达 6.3 亿。社会的发展，人民生活的提高，带动了汽车装备和加油站的发展。首先，高速公路建设发展迅速，到 1999 年底，达 1.1 万公里，仅次于美国（8.85 万公里）、加拿大（2 万公里）和德国(1.12 万公里),位居世界第四。2000 年底达 1.6 万公里，跃居世界第三，中国公路总里程达 130 多万公里。目前，全球机动车保有量为 8 亿多辆，其中美国达 1.5 亿辆以上。我国机动车保有量为 4000 多万辆（其中民用 1000 多万辆；北京市约 150 万辆，居全国之首），近几年以每年近 200 万辆的速度增长。1924 年，中国在上海建成第一座加油站。1949 年解放前夕，全国仅有 164 座加油站，集中在 7 座大城市。到 1984 年底，全国加油站达 2000 座。石油化工业日新月异，石油销售网点和加油站的建设发展迅速。目前，全国约有 10 万余座加油站。

尽管我国机动车、加油站如雨后春笋般地增加，但加油结算工具、手段和加油作业的控制管理方式进步不大，距离国外先进技术手段差距甚远。

信用卡交易手段于 1950 年产生于美国。50 多年来，已经开始在世界各地包括发展中国家普及。中国从 20 世纪 80 年代初开始，以“金卡工程”的名义，大力推广以磁卡为代表的信用卡、借记卡及其他形式的金融卡，以 IC 卡为代表的公益服务结算卡和管理卡、公交卡、加油卡、就餐卡、医疗卡、门禁卡、考勤卡、身份卡、水电气表卡等。到 2001 年 8 月，仅金融卡总发行量就达 3.3 亿张。

自 80 年代以来，不少地区开始试用磁卡加油。国家启动“三金”工程，特别是“金卡”工程后，各地不少石油公司和加油站点积极行动起来，进行了 IC 卡、卡机联动、联网结算、异地加油的试点。目前已经有 20 多个省、市开展了

加油卡应用的试点。

本书仅以加油IC卡的相关技术及其应用为重点，希望能对我国石油化工业加油站IC卡的应用尽微薄之力，供各级领导、加油站管理的业务人员、IC卡及其相关技术供应商、集成商和科研教育部门的有关人员参考。

由于本书涉及许多专业和学科，而且加油IC卡技术在我国刚刚应用，所以编写过程中错误难免，敬请专家指正。借此机会，对本书的编写出版和提供技术资料的北京握奇数据系统有限公司、福建实达电脑设备有限公司、北京航天金卡电子工程公司、北京捷德智能卡系统有限公司、金普斯公司、斯伦贝谢技术(亚洲)有限公司、明华澳汉科技有限公司、天津环球磁卡有限公司、北京长吉加油设备有限公司、北京北长空工业有限公司、北京北方正星数据技术有限公司、北京君汇博科发展有限公司、南京东富石油设备有限公司、香港百富科技有限公司、北京宇博电子科技有限公司及具有关人员表示衷心的感谢！

中国石油化工股份有限公司
信息系统管理部副主任　张志檩

2001年11月

前　言

随着目前国内汽车持有量的快速增长，为其提供服务的加油站也得到了快速的发展，并已基本实现了机械加油机向电脑加油机的升级换代，初步满足了目前汽车普及的需要。

随着加油站的普及，加油站之间的竞争也已经开始，尤其是随着成品油价格体系与国际市场的逐步接轨，改变了成品油价格一成不变的局面，由此对管理水平提出了更高的要求，但在结算形式上，除部分采用以油票为主体的预付费结算方式外，占主体的还是传统的现金支付方式，由此暴露出如下的问题：

① 急待加强业务数据的收集、汇总、分析能力，为销售决策提供依据。现代管理技术的发展，其核心就是计算机数据管理，没有准确、完备的基础数据，就难以保证管理水平的不断提高。由于加油站零售业务数据的统计汇总基本上还是以手工、半手工为主，数据的完备性、准确性、时效性不能满足提高业务管理水平的需要；

② 工作效率急待改进。由于目前支付方式主要是现金和纸制油票，因此，加油站基本还是以传统的加油工手工加油为主，劳动效率低，从业人员数量庞大；

③ 管理手段落后。由于以加油站为代表的管理环节中人为因素的影响，存在着相当大的管理漏洞，管理成本居高不下；

④ 传统的以纸制油票为代表的结算体系已难于适应市场的发展，急需一种适应上述变化的新型结算手段以提高服务水平，适应市场竞争的需要；

⑤ 资金安全问题比较突出。目前由于在加油过程大量使用现金进行交易，加油站又缺乏安全有效的保安措施，加之很多加油站位置偏僻、交通便利，所以存在很大的安全隐患。

由此可以看出，传统的结算方式，已成为制约加油站服务水平提高的重要瓶颈之一。从国际水平来看，自 1974 年 TOKHEIM 的第一部以 TTL 技术为主和 1975 年吉尔巴克（GILBARCO）公司的第一部以 4 位微电脑技术为主的电脑加油机问世以来，25 年来各种技术不断地被引进到加油机上，微电脑从 4 位到 32 位，显示器由简单的单行显示到防雨、防爆的大屏幕。近 20 年来，随着微电脑技术的进步和管理软件的普遍应用、通讯设备的技术完善与技术成本的降低，使得欧、美、日等发达国家的加油站管理与技术水平在解决了结算问题后，大幅提高，并向更高的层次发展。在最近几年，出现无线电加油机、机械人加油

机、具有油汽回收功能的加油机以及互联网加油机等新技术。投资在技术上的主要着眼点是用更好的服务来吸引更多的顾客，增加销售与市场占有率，提高公司的效益。同时，凭借技术的提高，减少由于人为和其他因素造成的库存问题，及时采集销售和市场的各种信息。

在结算方式方面，以美国一些世界级的大石油公司为代表，为了提高服务水平与方便客户，充分利用其发达的金融服务行业提供的、以信用卡为代表的信用体制的保护，于1990年初开始安装用磁卡加油的加油机，用户可以用威士卡(VISA)和万事达卡(Master Card)加油。目前在欧美和日本，一张威士卡已经可以在各地不同的加油站加油，真正达到一卡行天下的目的。只要您有一张威士卡或万事达卡，您就可以在欧美或日本任何一家有磁卡加油功能的加油站加油。用户直接将车开到加油机旁边，下车，插卡，系统立刻将卡上资料与个人密码(PIN)以加密方式，借助于卫星、专线或特殊系统送至数据中心，数据中心分析资料（检查黑名单等），检查用户的账户与其他资料，在4s内将授权返回加油机。加完油后，交易资料立即被转至数据中心，再转至银行结算中心或其他结算中心。用户的银行收到此资料后，立即与用户的账目作结算。目前在美国的大石油公司，几乎已经全部完成磁卡加油机的联网工作。并以此为基础，为解决由于人工费用的提高而导致的成品油毛利减少的问题，各大石油公司纷纷将加油站改成“自助加油”的方式。

由于国外加油站目前已建立起以应用金融卡联机自助加油为主体的技术发展方向，建立起了覆盖全部业务网点的计算机管理网络体系，因此目前正积极将互联网、无线通讯、现金自助加油等技术手段积极纳入到现有业务系统之中，并更加重视绿色环保技术的应用，以期进一步提高加油业务的自动化水平。

通过分析国外加油技术的发展轨迹，我们可以看出建立覆盖全部业务网点的数据采集汇总系统和向自助加油方式发展，是我们目前最急待解决的课题。国外以磁条卡技术为代表的加油系统是经过了几十年的发展建设，才达到目前的水平。在这个发展过程当中，以信用制度为代表的良好的金融环境和良好、廉价的通讯基础环境起到了重要作用。这些条件目前国内尚不完全具备。就现状而言，主要问题包括：信用制度尚处在发育期，银行卡的恶意透支行为频频发生；银行卡的普及程度还比较低，全国联网工作刚刚开始，交易速度比较慢，可靠性不高；通讯费用高昂，边远地区通讯基础设施薄弱等。因此，如果目前不加选择地照搬国外的成功经验，在短时间内取得成功可能会有较大的风险。反之，如果能更好地利用我们的后发优势，在充分学习分析国外成功发展的经验教训，结合我国的实际情况，采用能适应市场要求的新技术、新产品，采用跨越式发展的途径，才能使我们的零售领域在较短的时间内赶上国外几十年发展的水平。

智能IC卡技术的出现，为我们提供了一条跨越式发展的可行的解决途径。

智能IC卡技术是近年来随着超大规模集成电路技术的迅速发展，诞生并成熟起来的一项新技术，与磁条卡相比，具有安全性高、可脱机使用的优点。

虽然智能IC卡具有上述优点，但国外公司由于已在磁条卡上进行了大量投资，受投资的限制，目前很难迅速向IC卡技术升级。但对于尚处于起步阶段的国内加油行业来说，这些优点则非常适合国情的需要。因此，自1998年中国人民银行制订发布了《中国金融集成电路(IC)卡规范》以来，智能IC卡在国内各个应用领域的应用取得了迅猛的发展。

智能IC卡在加油领域应用时，首先根据加油消费的特点，即加油消费是先付货后付费，而金融消费是先付费后付货，来制定相应的解决方案——灰锁方案，以保证交易资金的安全，这就需要制定专门的卡片操作技术规范，并委托智能IC卡操作系统COS厂商开发出相应的技术产品。其次，加油IC卡的成功应用需要一整套的相关产品技术的支持，如：安全认证模块SAM技术、直接操作智能IC卡的各种终端设备技术、用于事先对智能IC卡进行处理的发卡设备技术，还包括最重要的、直接完成加油消费过程的卡机联动加油机及其改造技术等。有了上述产品技术的相互配合，才能保证加油IC卡应用的完成。除了具有上述产品技术外，还需要借鉴目前比较先进的国外磁条卡加油系统建设的成功经验，开发一整套应用上述技术的、网络化的计算机应用系统，实现智能IC卡应用各个环节的有效管理，真正发挥出加油IC卡应用的整体优势，并带动国内加油环节的技术服务水平，向更高的层次迈进。最后，加油IC卡只有推广到地域范围广阔的应用环境中，才能真正反映出其技术优点，而这一环境的建立，往往需要与银行进行相应地配合，并需要一整套的系统安全管理技术和方法。随着智能IC卡技术的进步和加油IC卡的普及推广，在解决了加油环节的应用之后，还可以把智能IC卡技术应用到从油品的采炼、配送等更加广阔的方面，以期充分发挥智能IC卡设备的投资效果，相应降低系统总体的造价。

总之，只有将加油IC卡当作一项系统工程来进行开发、建设和应用，才能真正解决支付手段问题，为加油行业的持续技术进步和服务水平的不断提高提供一个广阔的发展空间，并在我国加入WTO后不可避免的与国外加油企业的直接竞争中，处于不败之地。应用智能IC卡及其在此基础上发展起来的卡机联动技术，可有效降低系统造价，提高系统建设速度，取得事半功倍的效果，是提高竞争能力的有效手段。其意义主要体现在：方便客户和增强企业竞争力这两个方面。

1. 方便客户

应用加油IC卡，可为客户提供了安全、快捷的加油方式，插卡即用，拔卡即走，提高加油效率，减少顾客等候时间；

应用加油IC卡，可省去客户携带大量现金和油票的不便，做到“一卡在手，各地加油”；

应用加油IC卡，安全可靠，可重复储值、查询、挂失，增加客户的安全感；

应用加油IC卡，对单位客户在保持与纸制油票相同的结算方便性的同时，便于加强单位用油管理。

2. 增强企业竞争力

实施IC卡加油后，通过新技术手段的使用，改善了微观管理，尤其是加强了对加油工工作的管理。加油IC卡系统的建立，在防止不规范行为、降低经营风险的同时，也为业务管理信息系统提供快速准确的销售信息，为企业经营决策提供可靠的依据，提高经营决策的科学水平。通过加油IC卡进行电子结算，减少现金数量，保证资金安全，加速资金周转。加油IC卡应用的普及，为实现加油自动化，发展自助加油站，提高工作效率，提供了可靠的保证。加油IC卡的推广，实现“一卡在手,各地加油”,可扩大企业的知名度和零售市场占有率，提高企业的市场竞争能力。

目录

第一章　磁卡与IC卡技术

使用卡片作为个人身份识别的手段，具有悠久的历史。如现在常见的名片，由于卡片作为一种身份标识的手段，所体现出的方便性，人们很容易就想到使用它做为交易的凭证。随着技术的发展，人们乐于使用当时最先进的技术手段对它不断进行改进，使它具有了越来越重要的作用。

第一节　卡片技术与应用的发展

早在19世纪80年代，使用卡片作为交易凭证，就萌芽于英国，初期是使用纸制卡式凭证。到1915年，美国的一些商店和饮食店为了招揽生意，创造了一种“信用筹码”，开始使用一种金属徽章，后来又随着化学工业的发展演变成塑料卡片，作为顾客购物消费的凭证，持卡人可以先消费或赊购而事后付款。

1950年美国商人设计了第一张现代的塑料信用卡。1951年美国富兰克林银行作为金融机构率先发行了信用卡，并在50年代，出现了冲压出凸字的塑料卡，如一种主要用于金融交易的塑料金属交易卡，即FTC(financial transaction card)。它可以使用简单的机械方法把记载卡片发行者和客户帐号的凸字印在纸制凭证上，并很快在航空、旅游和娱乐业获得广泛应用。

20世纪60年代末，随着计算机的应用和磁记录技术的出现，人们很快在FTC卡的背面贴上磁条，发展成能自动读取信息进行在线计算机自动处理的磁卡，也就是今天人们还在使用的磁卡。70年代至80年代是磁卡技术的发展与应用的鼎盛时期，特别是在美国，据1988年的材料统计，已发磁卡10亿张，人均达到5张卡。

磁卡具有很多优点，主要是易读写、易修改、易复制，这些特征给用户和开发人员带来了许多方便，但也正因为这些特征，使得磁卡本身的信息具有易消失、易伪造等不可靠和不安全因素，从而限制了磁卡技术的进一步发展和应用。

在这种背景下，人们迫切需要新型卡片的出现，并寄希望于最新的超大规模集成电路技术，于是在卡上镶嵌有集成电路IC芯片的IC卡诞生了。

一、IC卡的起源

IC卡(integrated circuit card)，正式名称应叫集成电路卡，是将一个专用的集成电路芯片镶嵌于塑料基片中，封装成卡的形式。由于IC卡具有一定的数据处理能力，所以又叫智能IC卡、灵通卡等。

IC卡最初出现于法国。1970年法国新闻记者罗兰·莫雷诺提出了将一个集成电路芯片镶嵌在一块塑料卡上的想法，并随后在1972年做出了一张卡，这就是世界上第一张IC卡。

1976年法国布尔(Bull)公司高级研究员Ugon先生领导的研究小组首先研制了世界上第一个由两个集成电路(微处理器和存储器)芯片组成的IC卡，接着又于1978年制成了单芯片的智能IC卡，并取得了技术专利，由此奠定了以法国为代表的欧洲在IC卡领域的地位。

1985年以来，世界著名的万事达(master card)信用卡公司在美国对法国的IC卡进行了现

场测试，获得满意的结果，此后，IC卡就以更大的规模在更广泛的领域上发展和应用起来。

从目前情况来看，法国是使用IC卡最多的国家，并形成了自己的发展模式。而美国由于已广泛使用磁卡，建立了世界上最完善的信用制度，加上受投资问题的制约，很难全部迅速改用IC卡。日本在IC卡应用方面有相似的问题。

到90年代初，世界上先后有德国的西门子Siemens(现亿恒 Infineon 公司)、法国的 Thomson、美国的 Motorola 和 Atmel、荷兰的 Philips、日本的日立等半导体公司或厂家，都投入了IC卡芯片的开发和生产。

从1987年开始，国际标准化组织ISO制定和颁布了IC卡的第一个国际标准——ISO/IEC 7816，为IC卡的进一步发展和普及创造了条件。

IC卡诞生后，随着集成电路技术的迅速发展，其性能价格比迅速提高，在实际应用中，体现了与磁条卡相比信息存储量大、安全性好的优点。除传统的接触通讯方式之外，还出现了能够进行无线通讯的非接触式卡片，应用范围也从传统的交易凭证扩展到更广阔的领域。

在IC卡的发展应用过程中，根据各种应用环境的不同要求，产生不同形形式的IC卡。为了满足一些对安全性要求不高的应用环境，产生了只有简单控制电路和存储器的存储卡，由于芯片结构简单，成本大大降低，对IC卡的应用普及起到了推动作用；为了满足各种门禁、交通等应用要求，产生了支持采用无线通信技术的非接触式卡片，提高了卡片和机具在恶劣应用环境下的可靠性，提高了操作效率；为了满足一些对操作速度要求很高的应用要求，产生了带有专用硬件算法协处理器的高速IC卡。为了满足高安全性要求的应用，提供数字签名的功能，初期卡片内部的对称密钥算法已无法满足要求，于是产生了支持公开密钥算法的IC卡。

二、IC卡的分类

在IC卡出现后，与磁卡相比，由于其具有一定的运算处理能力，于是人们就自然地给它起了个形象的名称——智能IC卡。虽然大家见到的IC卡外观基本都差不多，但其实它可以根据不同划分方式，划分为不同种类。

1. 按通讯方式划分

根据通讯方式的不同，IC卡可分为接触式IC卡、非接触式IC卡及双界面卡三类。

接触式IC卡通过ISO/IEC 7816国际规范要求的8个接触点，在卡与卡的读写机具之间进行信息交换。

非接触式IC卡在卡片的卡基内嵌有一组特别的感应线圈，当卡片靠近读写机具时，机具内发出的特别的射频载波在卡片的感应线圈周围形成一个交变磁场，通过耦合产生电势能，并驱动卡与机具进行通讯。

双界面卡(dual interface,简称DI)同时支持上述两种通讯方式，最初是在卡内同时封装一个接触芯片和一个非接触芯片构成，由于两个芯片之间不能直接共享彼此的数据，使用不方便，其后又出现了只用一个芯片就能同时支持两种通信方式的单芯片双界面卡。由于两种通讯方式由同一个芯片实现，因此大大方便了使用，现在通常所提的双界面卡，如非特别说明，一般都指后一种。

2. 按结构划分

根据智能IC卡的内部结构与技术特性的不同，可以分为存储器卡(memory Card)和微处理器卡(CPU card)两大类。这两类IC卡的最重要区别在于存储器卡内不含有微处理器，仅具有一般的数据信息的存储功能。

(1) 存储器卡

存储器卡又可分为：普通存储器卡和逻辑加密卡。它们主要被应用于保密性要求不高的信息存储和小额预付费卡等。

普通存储器卡的内部结构仅为一块 EEPROM 存储区，只提供读写两种操作功能，基本安全性为：认证密码及熔丝保护。一旦卡片认证通过，即可对整个存储区自由读写。其典型的应用为公用电话 IC 卡。

逻辑加密卡与普通存储器卡相比，内部结构较为复杂，其存储区可以分成卡片设置区和应用区。卡片设置区内存放与卡片厂商及发卡者相关代码和卡片密码；应用区又可以根据需要分为不同的分区。逻辑加密卡的安全性相对提高，主要体现在：卡片设立主密码、每个应用分区具有各自独立的操作密码、由加密逻辑电路控制读写操作、设立认证错误计数器等。

对于存储器卡而言，即使是逻辑加密卡，其自身的安全控制能力都是低层次、非常有限的。它一般仅能控制数据是否可以写入，但无法保证写入卡内数据的完整性与可靠性，无法防止外部对卡片的恶意攻击。在此情况下，存储卡通常只适合记载一些比较固定的信息，如卡号、持卡人资料、账号等，对于涉及敏感数据或涉及支付的应用系统中，在使用存储器卡时往往采用与磁条卡相似的联机操作的方式，即把上述重要信息记载在系统的主机当中，卡片仅仅起到持卡人身份标识作用，支付信息直接记录在系统主机中。

上述使用方法，借鉴了磁条卡的应用模式，但不能有效避免伪卡的产生，一旦卡片结构和仅有的密钥被别人获知，可以比较容易地制造伪卡，系统难于防范。由于在通讯中传输的数据主要是通过明文方式进行，因此只要采用搭线窃听方式，配合一些比较简单的设备，专业人员就可以获得上述信息。

在上述应用方式中，由于每次交易均需支付通讯费用，且建立较大范围、尤其是以全国通用为目的、支持实时联机交易的通讯网络成本高昂，对于交易金额较小的应用，经济上难于承受。

此外，在存储卡类型的卡片中，还有一类特殊的卡片——计数卡，如大家常见的电话 IC 卡，卡片内部主要包括一个只能进行减数操作的计数器，直到计数器的数字减到 0 为止。计数卡同样存在比较容易产生伪卡的缺点，因此一般只用于很小金额的消费应用领域。

(2) 微处理器(CPU)卡

严格地说，只有微处理器卡才具有数据处理功能，才是真正的智能 IC 卡。因此，在本文中所称的智能 IC 卡专指带有微处理器的 IC 卡。顾名思义，微处理器(CPU)卡的芯片中不仅有存储单元 EEPROM，还含有 CPU、ROM、RAM、运算协处理器以及相应的芯片操作系统(COS - chip operating system)和输入输出(I/O)端口等，相当于一台微型计算机，只是没有显示器和键盘。在 COS 的控制下，智能卡拥有树状的文件目录结构、一套包括卡片管理和应用的指令集、密码 + 密钥为主的较高的安全保密机制、数据加密与认证以及异步 I/O 通讯协议，可以实现：存储器管理；文件管理；I/O 控制与处理；逻辑计算能力；加/解密、安全认证的运算功能等。这种微处理器卡可应用于几乎所有的领域(典型的应用：电信 SIM 卡、金融支付卡、身份认证卡等)。

与存储器卡相比，智能卡的突出优点体现在：拥有芯片操作系统(COS)和高级别的安全保密机制与加密算法。因此，智能卡可以做到：提供基于密钥的安全策略(密钥分散、过程密钥，文件访问控制…)；对卡内的敏感数据加密存储；提供对外部世界(接口设备、IC 卡、持卡人…)的相互认证手段；设置为保护敏感数据传输可靠性和完整性的报文鉴别码(MAC)；