智能卡研发技术与工程实践

求是科技　李翔　编著

人民邮电出版社

前　言

随着芯片技术的发展和应用安全性要求的提高，IC 卡作为一种新兴的应用平台，在诸多领域中有着十分广泛的应用，如金融、社保、市政、加油等。在 IC 卡系统中，卡片内的操作系统 COS 是整个系统的核心，它的设计与开发既要遵循一定的规范，又存在很大的灵活性。

编写本书的目的就是将笔者多年来设计和开发 COS 的相关经验加以总结归纳，本着将理论知识和应用相结合的思路，系统详尽地介绍 COS 系统设计和开发过程中常见的问题，并且给出解决方案的实例，希望本书能够给广大的 IC 卡设计开发人员以参考。

本书共分 13 章，下面简单概述各章的内容。

第 1 章：初始 IC 卡

本章首先介绍了 IC 卡发展的历史及其在国内外的应用现状，然后重点介绍了 IC 卡的主要应用领域及其应用特点，最后引入了 IC 卡系统中最重要的部分——卡内操作系统（COS），详细介绍了 COS 的主要功能和发展现状。熟悉和掌握这些内容有助于从整体上了解和把握 IC 卡的特点和应用要求。

第 2 章：COS 开发的预备知识

本章重点分析了 COS 系统的需求，并且对 COS 系统的结构进行了初步设计。首先介绍了如何进行 COS 的需求分析，包括了应用、环境、存储、安全等多个方面；然后介绍了进行 COS 系统开发前需要掌握的相关知识；接着简单给出了 COS 开发的通用流程；最后按照功能将 COS 系统划分为 4 个层次和 4 个主要功能模块。通过本章的学习，读者将能够对 COS 功能及其开发有一个总体的了解。

第 3 章：IC 卡芯片

本章首先详细介绍了 IC 卡芯片的种类和逻辑结构，主要包括了 8 个逻辑模块；然后根据这些逻辑模块逐一介绍了在不同的应用需求下模块的功能要求及芯片的选型原则；最后以 ST 公司的系列芯片为例介绍了 3 类面向不同应用需求的芯片性能。

第 4 章：IC 卡的传输协议

COS 的 I/O 模块是最基础的模块之一，该模块的功能要求遵循传输协议的定义。本章首先介绍了 IC 卡的操作过程，包括正常流程和异常中断的处理；然后介绍了一个字符的物理传送过程，这是 IC 卡数据通信的基础；接下来介绍了 IC 卡的上电复位应答；最后给出了通用的 IC 卡传输协议，包括 T＝0 和 T＝1 两种类型，可以划分为物理层、数据链路层、终端传输层和应用层等。

第 5 章：IC 卡的文件系统

本章首先介绍了 IC 卡内文件系统的组织形式，包括文件系统的逻辑结构和对文件系统的操作；然后介绍了卡内存在的 3 种文件类型，并且给出了在实际应用中可能碰到的文件系统

逻辑结构示例；接下来设计了一个简单的文件系统在卡内的存储机构，包括文件头和文件体两个部分；最后根据文件操作的需要，设计了 7 条文件操作命令。

第 6 章：IC 卡的安全体系

IC 卡的安全体系是 COS 系统的核心模块。本章首先介绍了 IC 卡的安全结构，包括安全属性、安全机制和安全状态 3 个部分；然后分别介绍了在卡内安全模块中可能涉及的几个安全算法，包括算法原理和部分算法实现代码；接下来给出了一个卡片安全结构设计的示例，建立了一个简单的卡片安全环境；最后根据安全操作，设计了 8 条相关命令。

第 7 章：多应用 IC 卡的实现

本章首先介绍了 IC 卡的生命周期，包括 IC 卡的使用流程和卡片的生命周期状态；然后介绍了 IC 卡的应用模式，在不同的应用模式情况下，IC 卡系统中不同的角色定义和角色之间的关系转换；接下来介绍了在多应用环境下卡片状态的维护，并且给出了一个多应用 IC 卡设计的示例，包括卡片生命周期的维护、应用之间的保护机制和安全状态的维护机制等；最后根据应用维护操作的不同，设计了 5 条相关命令。

第 8 章：COS 的工作流程

本章以实例的形式重点介绍了 COS 在实际运行过程中涉及到的 4 个主要流程的工作原理，这 4 个流程分别是主守护流程、数据 IO 流程、命令处理流程和数据安全写流程。通过对这几个流程分析，读者能够基本掌握 COS 的整体结构和运行情况。

第 9 章：中国金融集成电路卡应用

本章重点介绍了 IC 卡应用领域的一个最重要的应用，也就是金融卡应用。首先介绍了金融卡应用的基本情况，给出了应用的文件系统设计；然后介绍了金融卡应用规范定义的 13 条命令接口、卡片在使用过程中应用状态的维护情况和卡片的安全结构设计要求；接下来给出了卡片在实际使用过程中的 10 个主要交易流程；最后根据交易流程简单介绍了卡片命令在这些交易流程中的组合使用情况。

第 10 章：社会保障卡应用

本章重点介绍了 IC 卡应用领域的另一个最重要的应用，也就是社会保障卡应用。首先介绍了社会保障卡应用的基本情况，给出了应用的文件系统设计；然后介绍了社会保障卡中医疗保险应用规范定义的 8 条命令接口、和卡片的安全结构设计要求；接下来给出了卡片在实际使用过程中的 10 个主要交易流程；最后根据交易流程简单介绍了卡片命令在这些交易流程中的组合使用情况。

第 11 章：中国石化加油集成电路卡应用

本章重点介绍了中国石化加油集成电路卡应用。首先介绍了加油卡应用的基本情况，给出了应用的文件系统设计；然后介绍了加油卡应用规范定义的 18 条命令接口、卡片在使用过程中应用状态的维护情况和卡片的安全结构设计要求；接下来给出了卡片在实际使用过程中的 13 个主要交易流程；最后根据交易流程简单介绍了卡片命令在这些交易流程中的组合使用情况。

删除的内容: 读
删除的内容: 了
删除的内容: 三
删除的内容: 重
删除的内容: 四
删除的内容: 、
这四个流程的
例及在这些示
有关数据结构
删除的内容: 四

第 12 章：支持公钥应用的公钥卡

本章介绍了目前最为流行的一个 IC 卡应用，也就是公钥卡应用。首先介绍了公钥（PKI）体系的基本情况，包括 PKI 体系的结构、工作流程及安全分析；然后介绍了 PKI 相关的主要算法原理，包括加密算法和签名算法两大类；接下来根据 IC 卡的实际情况对 PKI 算法在卡内的实现进行了选择，简单设计了一个 PKI 卡的文件结构和 PKI 主要流程在卡内的实现流程；最后设计了 PKI 相关的 9 条命令。

第 13 章：智能卡应用解决方案示例

本章主要介绍了智能卡应用的整体解决方案，包括这些解决方案设计的应用领域的基本情况介绍、相关系统的结构设计、卡片在该系统中的主要功能、以及系统相关软硬件的配置要求等，这些系统包括了校园一卡通应用、社会保障卡应用和网吧监管系统应用，通过这些应用方案，读者能够对 IC 卡的实际应用有一个整体的把握。

附录部分主要提供了在本书中涉及的专用命令及其缩写，以便读者查阅。

由于作者水平有限，书中难免有不足和疏忽之处，恳请读者朋友和各位同仁批评指正。读者通过访问求是科技的网站 http://www.cs-book.com，可以下载到本书所涉及的代码。并欢迎对本书的问题和不足提出您最宝贵的建议和意见，同时，在“求是论坛”上还可以进行智能卡的相关技术交流。

编者

2003 年 10 月 于清华园

删除的内容: 前

删除的内容: 和

删除的内容:

删除的内容: 第

缩略词列表

删除的内容: 本

删除的内容: 总

删除的内容:

删除的内容:

读者通过访问

网站www.cs-b

以下载到本书

码。并欢迎对本

不足提出您最

和意见。在求是

以进行智能卡

交流。

在此，感谢人民

的信任和支持

删除的内容: 作

删除的内容: 2

删除的内容: 于

目　录

第 1 章　初识 IC 卡

本章主要介绍 IC 卡的一些背景知识，让读者对 IC 卡及其应用情况和卡内操作系统（Chip Operation System，简称 COS）有一个初步认识，主要包括如下几项内容：

- IC 卡发展的历史。
- IC 卡国内外的应用现状。
- IC 卡的主要应用领域。
- 卡内操作系统的基本概念。
- 卡内操作系统的发展现状。

1.1　IC 卡的发展与现状

1.1.1　IC 卡的发展历史

1970 年，法国人罗兰德·莫瑞诺（Roland Moreno）第一次将可进行编程设置的 IC（Integrated Circuit）芯片放于卡片中，使卡片具有更多的功能。当时他在专利申请书中，对这项发明作了如下阐述：卡片上具有可进行自我保护的存储器。这样就诞生了世界上第一张 IC 卡。在此后的时间里，随着超大规模集成电路技术、计算机技术以及信息安全技术的发展，IC 卡技术也更趋成熟，它的发展经历了多个重要阶段，其技术也在不断地进步。

智能卡属于半导体卡，半导体卡片采用微电子技术进行信息的存储、处理。按照其组成结构，智能卡可以分为一般存储卡、加密存储卡、CPU 卡和超级智能卡等。

- 一般存储卡（Memory Card）

一般存储卡也叫非加密存储卡，其内嵌芯片相当于普通串行 EEPROM 存储器，有些芯片还增加了特定区域的写保护功能，这类卡存储信息方便、使用简单、价格便宜、很多场合可替代磁卡，但由于其本身不具备信息保密功能，因此，只能用于保密性要求不高的应用场合。

- 加密存储卡（Security Card）

加密存储器卡内嵌芯片在存储区外增加了控制逻辑，在访问存储区之前需要核对密码，只有密码正确，才能进行存取操作，这类信息保密性较好，使用与普通存储器卡相类似。但是密码一般通过明文进行传递和验证，很容易被破解，一般用于需要进行简单保密要求的应用场合。

- CPU 卡（Smart Card）

CPU 卡内嵌芯片相当于一个特殊类型的单片机，内部除了带有控制器、存储器、时序控制逻辑等外，还带有算法单元和操作系统，由于 CPU 卡有存储容量大，处理能力强，信息存

储安全等特性，因此，被广泛用于信息安全性要求特别高的场合。

- 超级智能卡（Super Smart Card）

在卡上具有 MPU 和存储器并装有健盘、液晶显示器和电源，有的卡上还具有指纹识别装置等，主要用于高端应用。其核心和 CPU 卡类似，主要增加的是外围的辅助单元。

CPU 卡的出现是 IC 卡发展史上的重要阶段，区别于它的前身——加密存储卡，其芯片具有更强的数据处理能力，能够在卡内完成复杂的数据运算和逻辑控制，从硬件底层提供了对数据和应用强大的安全保护能力，逐步成为了卡应用的主流，本书将要介绍的就是 CPU 卡（根据不同区域场合，也称为智能卡、IC 卡、聪明卡等）。

按照卡片数据的读写方式，智能卡又可分为接触式 IC 卡、非接触式 IC 卡和双界面卡 3 种类型。

- 接触式 IC 卡

由读写设备的触点和卡片上的触点相接触才能够进行数据读写。

- 非接触式 IC 卡

卡片使用过程中与读写设备无直接的电路接触，由无线非接触技术进行读写（例如，光或无线电技术等）。和接触式 IC 卡相比较还增加了射频收发电路，这类卡一般用在使用频繁、使用要求便利的场合。

- 双界面卡

双界面卡综合了以上两种读写技术于一身，既能够提供接触式读写方式，也能够提供非接触式读写接口，方便用户在不同场合使用卡片的不同需求。

智能卡的出现是微电子、计算机和信息安全等多学科技术综合的结果，作为一种成熟的高技术产品，智能卡的广泛使用将能够提高人们生活和工作的现代化程度，这已成为一个国家科技发展水平的标志之一。

1.1.2 IC 卡在国外的应用情况

在 1988 年 10 月至 1989 年 9 月期间，全世界 IC 卡和读写器数量已分别达到 4200 万张和 37700 台，其中法国分别占 98%及 71%，处于世界领先地位。据智能卡月刊（Smart Card Monthly）统计，目前每年的 IC 卡产量突破 4 亿张（其中 CPU 卡所占的比重不低于 50%），IC 卡和 IC 卡处理设备总产值均突破 15 亿美元。这些卡的使用，必然遍布人类生活的各个领域，也必然涉及到数以千计的工程，还有服务、咨询等方面的业务，整个智能数据卡的市场将是巨大的。

新一代智能卡将以储值卡为主，主要应用领域包括 Internet 购物、商店售货亭、移动电话卡、家庭电视付费点播卡等。另外用于存储媒体信息和个人信息的数据卡也将有比较显著的增长。

从具体应用领域来讲，在金融领域世界上最大的信用卡集团 VISA 卡集团，为扩展金融服务范围，满足未来金融服务的需要及提高安全性，开始准备转向智能卡。VISA 还和 MasterCard 以及 Europay 共同制定新的国际银行交易标准，这将极大拓展世界性的智能卡应用范围。

医疗事业领域，法国将在所有医疗事业发行单一的国家智能卡。为从根本上改善法国全国的国有医疗系统的有效性及高效性铺平道路，这种智能卡还将朝着健康医疗信息技术方向

发展，甚至还将在国际范围内寻求合作。

还有包括交通运输，校园管理及军人身份证方面的应用，正是由于各种智能数据卡应用的迅猛发展，可以肯定世界智能数据卡近年内将会有突破性的增长。

1.1.3　IC 卡在国内的广泛应用

1993 年 6 月江泽民主席针对我国存在的大量现金发行、资金体外循环以及经济犯罪等问题，为稳定金融秩序、加强国家对经济的宏观控制、加速金融商贸现代化建设，倡导在全民推广使用信用卡。同年 9 月国家金卡工程正式启动。

金卡工程的主要任务是推行电子货币，实现支付手段的革命性变化，为个人和企业提供方便、快捷、安全的支付手段，促进市场繁荣、经济发展，也进一步促进其他行业管理现代化，加速国民经济信息化进程。城市现代化进程中的一个重要标志就是城市的信息化建设，要在社会上建立起一个高效、准确的信息采集和处理平台，满足未来社会对信息采集、分析、存储、查询等过程简练、快捷、准确的要求。目前，随着网络化的进程和电子商务的飞速发展，IC 卡作为一种成熟的电子支付手段也越来越受到业内人士的关注。智能卡技术的日趋成熟，也使得其在电子商务中的实际应用成为了可能，同时也使得电子商务更加简便易行，具有更强的安全性和保密性。

我国 IC 卡的大规模应用首先是在移动通信网上，从广东、上海建立中国最早的无线数字电话系统开始，随着手机在全民中极大普及，SIM 卡的发卡量从最初的百万增加到现在的数以亿计。在其他不同的行业，针对自身的应用特点，许多公司都纷纷推出了自己的行业 IC 卡解决方案，相关的监管部门也纷纷制定了本行业的卡应用规范，例如中国人民银行的金融 IC 卡规范、中国石化的加油卡规范、社会保障部的社保个人卡规范等，针对目前市政 IC 卡应用迅速发展的趋势，制定集合交通、水、电、煤气、门禁等多种应用的建设部指导规范也在紧锣密鼓的进行中。

从长远的来看，IC 卡的应用将具有如下的主要特点。

- 无论是小额消费还是全面替代信用卡，IC 卡都具有无以匹敌的优越性。
- 身份认证功能更突出，无论是金融还是非金融应用，身份识别都成为系统要解决的首要问题，而这一切在 IC 卡的参与下将变得简洁准确。
- 一卡多用。越来越多行业专用卡的出现将使得用户面临着一个新的烦恼，而卡容量的快速发展也使得那些单一用途卡的空间出现极大的浪费，技术上要解决的首要问题也就是如何在保证系统安全性的基础上有效地利用这些资源。
- 个性化的服务。随着社会的进步，人们要求的服务质量也越来越高，利用 IC 卡如何建立面向用户的个性化服务已成为目前业内关注的一个热点。
- 更高的安全性。随着科技的进步和 IC 卡应用范围的扩大，针对 IC 卡芯片硬件和软件攻击方面的研究就一直没有停止过，虽然目前的工艺技术能够抵御现有的攻击的手段，但是追求更高的软硬件安全保障机制一直是开发人员追求的重要目标。

也就是说，在未来的 IC 卡应用发展过程中，一个很重要的课题就是如何在技术上有效地发挥 IC 卡的优势，为构建完善的应用系统提供强有力的支持。