

全国高职高专教育电子电气类专业规划教材  
国家精品课程配套教材

# 智能卡 与RFID技术

■ 毛丰江 主编  
夏继媛 副主编



全国高职高专教育电子电气类专业规划教材  
国家精品课程配套教材

# 智能卡与 RFID 技术

Zhinengka yu RFID Jishu

毛丰江 主 编

夏继媛 副主编



高等教育出版社·北京  
HIGHER EDUCATION PRESS BEIJING

## 内容提要

作为物联网的关键技术之一,智能卡与RFID技术已形成涉及全球众多电子巨头的新兴技术产业,并普及到现代经济和日常生活的各个方面。

本书以4种典型产品为教学内容的载体,按3步工作流程来设计教学情境和组织教学内容,全面将智能卡与RFID的理论和实用技术融合于工作任务的完成过程中。本书分6章,第1章建立智能卡与RFID技术基础,第2~5章通过完成智能卡网吧收费机、智能射频卡公交收费机、智能卡电子钱包终端和RFID电子车牌识别系统等产品设计任务来学习接触式逻辑加密卡、智能(CPU)卡、高频及超高频RFID等应用技术,第6章则从应用系统角度加以综合。

本书为国家精品课程“智能卡技术”的配套教材,可作为高职、高专、成人教育电子信息工程技术、应用电子技术、自动控制技术、计算机应用技术及物联网技术等电子信息相关专业的教材,也可作为智能卡与RFID行业技术人员、系统集成商、系统用户及信息化工作者的参考书。

## 图书在版编目(CIP)数据

智能卡与RFID技术/毛丰江主编. --北京:高等教育出版社,2012.7

ISBN 978-7-04-035480-5

I. ①智… II. ①毛… III. ①IC卡-技术-高等职业教育-教材 ②无线电信号-射频-信号识别-高等职业教育-教材 IV. ①TN43 ②TN911.23

中国版本图书馆CIP数据核字(2012)第141104号

策划编辑 孙薇

责任编辑 孙薇

封面设计 于涛

版式设计 于婕

插图绘制 宗小梅

责任校对 李大鹏

责任印制 张福涛

出版发行 高等教育出版社

社址 北京市西城区德外大街4号

邮政编码 100120

印刷 北京印刷集团有限责任公司印刷二厂

开本 787×1092 1/16

印张 16.75

字数 410千字

购书热线 010-58581118

咨询电话 400-810-0598

网址 <http://www.hep.edu.cn>

<http://www.hep.com.cn>

网上订购 <http://www.landaco.com>

<http://www.landaco.com.cn>

版次 2012年7月第1版

印次 2012年7月第1次印刷

定价 26.50元

本书如有缺页、倒页、脱页等质量问题,请到所购图书销售部门联系调换

版权所有 侵权必究

物料号 35480-00

# 前 言

近年来,智能卡与 RFID 技术发展迅猛,业已形成一个涉及全球众多著名电子巨头的新兴技术产业,其应用范围遍及电信、金融、商业、交通、医疗、税务、身份认证及供应链管理、工业生产和安全管理等诸多领域。因此,需要大量精通智能卡与 RFID 技术的人才来从事各类智能卡及 RFID 配套设备和应用系统的设计、开发、制造、发行、维护和服务工作。为了适应高职院校开设相关课程的需要,结合近年来的技术发展和教学经验,我们组织编写了这本教材。

本教材为国家精品课程“智能卡技术”的配套教材,完全按照精品课程的工学结合课程模式来编写。根据行业的主流核心技术将课程内容分为4大模块(第2~5章),包括接触式逻辑加密卡技术、非接触式 IC 卡与 RFID 技术、智能(CPU)卡技术及射频识别(RFID)技术,对应选取应用广泛、技术实用、拓展性强的4种实用产品作为这4大核心技术的教学内容。同时以基本原理模块(第1章)为基础,以应用系统模块(第6章)为综合及与后续课程的衔接,全面贯穿于4项技术的应用过程中。

在4大核心技术模块中,我们以产品设计任务作为课程设计任务,在每个模块一开始就以系统需求分析的方式引入该任务,然后按产品开发流程把每一个课程设计分解为“卡的认识与操作”、“硬件设计与测试”、“软件设计与调试”3类技能训练项目,即“做一做”;让学生通过项目训练来掌握“卡的存储结构与安全特性”、“硬件电路工作原理”、“读写时序与软件编程”3种必备知识,即“学一学”。最后通过拓展来引导学生自主学习、研究本模块的其他相关技术和应用。

本书参考学时在60~90之间(含实训),可作为高职高专电子、计算机及物联网技术专业智能卡与 RFID 技术课程的教材,也可作为智能卡与 RFID 系统开发、制造、使用和维护人员的培训用书,使用者可根据具体情况增减学时。

毛丰江对本书的编写思路与大纲进行了总体策划,指导全书的编写,对全书统稿,并编写了第1、2、4、5章。夏继媛协助完成上述工作,并编写了第3章,王永兴编写了第6章。全书由毛丰江担任主编。

深圳明华澳汉科技股份有限公司、深圳达实智能股份有限公司、深圳新力量通信技术有限公司为本书的编写提供了很大的帮助,在此表示深切的感谢。同时,本书在编写过程中参考了大量国内外书籍、刊物、网站及培训资料,在此向这些资料的作者一并表示感谢。

在编写本书的过程中,我们力图全面反映智能卡与 RFID 技术各方面的知识、理论、技术和实践经验,但由于智能卡与 RFID 技术发展日新月异,限于编者的水平和视野,本书的不足之处在所难免,殷切希望专家和广大使用者对本书提出宝贵的意见和建议。

课程组与企业合作开发了与教材配套使用的智能卡与 RFID 实训设备,可提供相关实训室建设、实训设备供应等方面的配套支持,同时也可对采用市售通用读写器及读写模块自行搭建实训设备的教师提供技术指导。

编者

2012年5月

于深圳职业技术学院

# 目 录

|                                 |    |
|---------------------------------|----|
| 第一章 智能卡技术入门 .....               | 1  |
| 基础1 什么是智能卡 .....                | 1  |
| 基础2 缤纷卡族 .....                  | 4  |
| 1.2.1 存储器卡与微处理器卡 .....          | 4  |
| 1.2.2 接触式与非接触式 IC 卡 .....       | 5  |
| 1.2.3 RFID 电子标签 .....           | 7  |
| 基础3 智能卡的用卡过程与优势 .....           | 8  |
| 1.3.1 智能卡的设计制造和应用过程 .....       | 8  |
| 1.3.2 智能卡的使用流程 .....            | 10 |
| 基础4 智能卡的安全性 .....               | 13 |
| 1.4.1 威胁信息安全的因素 .....           | 13 |
| 1.4.2 智能卡的安全技术 .....            | 14 |
| 基础5 智能卡的标准 .....                | 16 |
| 1.5.1 智能卡的基本标准 .....            | 16 |
| 1.5.2 智能卡的应用标准 .....            | 17 |
| 1.5.3 智能卡的测试标准 .....            | 18 |
| 基础6 智能卡应用的发展趋势 .....            | 19 |
| 1.6.1 智能卡应用的地域趋势 .....          | 19 |
| 1.6.2 智能卡应用模式发展趋势 .....         | 19 |
| 思考题 .....                       | 20 |
| 第二章 接触式逻辑加密卡技术 .....            | 21 |
| 引入 智能卡网吧收费系统需求分析 .....          | 21 |
| 任务1 网吧卡卡型选择 .....               | 23 |
| 做一做 SLE4442 卡的读写操作 .....        | 24 |
| 学一学 接触式逻辑加密卡存储结构与安全特性 .....     | 28 |
| 2.1.1 接触式存储器卡的存储结构与安全特性 .....   | 28 |
| 2.1.2 接触式逻辑加密卡的逻辑结构 .....       | 29 |
| 2.1.3 逻辑加密卡的应用场合与代表产品 .....     | 30 |
| 2.1.4 SLE4442 卡的存储结构与安全特性 ..... | 31 |
| 任务2 智能卡网吧收费机硬件电路设计与测试 .....     | 33 |

|                                                |           |
|------------------------------------------------|-----------|
| 做一做 SLE4442 卡读写接口电路设计与测试 .....                 | 34        |
| 学一学 接触式逻辑加密卡读写接口电路与复位应答 .....                  | 37        |
| 2.2.1 接触式 IC 卡接口设备的硬件组成 .....                  | 38        |
| 2.2.2 接触式逻辑加密卡的复位应答 .....                      | 41        |
| 任务 3 智能卡网吧收费机控制软件设计与调试 .....                   | 43        |
| 做一做 SLE4442 卡读写软件设计与调试 .....                   | 43        |
| 学一学 接触式逻辑加密卡时序分析与读写程序 .....                    | 46        |
| 2.3.1 传送协议与操作模式 .....                          | 47        |
| 2.3.2 读卡(Read) .....                           | 50        |
| 2.3.3 写卡(Update) .....                         | 52        |
| 2.3.4 密码校验(Verify) .....                       | 53        |
| 拓展 其他类型的接触式逻辑加密卡及其应用 .....                     | 55        |
| 拓展 1 具有协议认证功能的逻辑加密卡 .....                      | 55        |
| 拓展 2 基于 TM 卡的小区巡检系统 .....                      | 58        |
| 思考题 .....                                      | 62        |
| <b>第三章 非接触式 IC 卡与 RFID 技术 .....</b>            | <b>63</b> |
| 引入 射频卡公交收费系统需求分析 .....                         | 63        |
| 任务 1 射频公交卡卡型选择 .....                           | 65        |
| 做一做 MIFARE 1 卡的读写操作 .....                      | 66        |
| 学一学 ISO/IEC14443 TYPE A 标准射频卡存储结构与安全特性 .....   | 69        |
| 3.1.1 非接触式 IC 卡系统的构成与特点 .....                  | 69        |
| 3.1.2 MIFARE 系列非接触式 IC 卡概述 .....               | 70        |
| 3.1.3 MIFARE 1 卡的存储结构 .....                    | 73        |
| 任务 2 射频卡公交收费机硬件电路设计与测试 .....                   | 77        |
| 做一做 ISO/IEC14443 TYPE A 标准射频卡读写接口电路设计与测试 ..... | 78        |
| 学一学 ISO/IEC14443 TYPE A 标准射频卡读写接口电路 .....      | 80        |
| 3.2.1 非接触式 IC 卡的信息与能量传递 .....                  | 80        |
| 3.2.2 非接触式 IC 卡与读写器的空中接口 .....                 | 81        |
| 3.2.3 非接触式 IC 卡读写芯片 .....                      | 82        |
| 任务 3 射频卡公交收费机控制软件设计与调试 .....                   | 87        |
| 做一做 MIFARE 1 卡读写软件设计与调试 .....                  | 88        |
| 学一学 ISO/IEC14443 TYPE A 操作流程与读写程序 .....        | 90        |
| 3.3.1 NXP MIFARE 读卡芯片寄存器剖析 .....               | 90        |
| 3.3.2 MF RC500 命令集 .....                       | 93        |
| 3.3.3 MIFARE 卡读写程序设计 .....                     | 96        |
| 拓展 其他类型的非接触式 IC 卡及其应用 .....                    | 103       |
| 拓展 1 非接触式 IC 卡的类型与国际标准 .....                   | 103       |

|                                |            |
|--------------------------------|------------|
| 拓展2 ISO/IEC 15693 协议及其应用 ..... | 107        |
| 思考题 .....                      | 110        |
| <b>第四章 智能(CPU)卡技术 .....</b>    | <b>112</b> |
| 引入 智能卡电子钱包系统需求分析 .....         | 112        |
| 任务1 电子钱包卡型选择 .....             | 114        |
| 做一做 CPU卡文件系统建立与文件读写操作 .....    | 114        |
| 学一学 CPU卡的构成与文件系统 .....         | 118        |
| 4.1.1 CPU卡的构成与特性 .....         | 118        |
| 4.1.2 CPU卡的文件系统 .....          | 125        |
| 任务2 电子钱包POS机硬件电路设计与测试 .....    | 128        |
| 做一做 SmartCOS卡读写接口电路设计与测试 ..... | 128        |
| 学一学 CPU卡的读写接口电路与数据传输 .....     | 131        |
| 4.2.1 CPU卡的读写接口电路 .....        | 131        |
| 4.2.2 CPU卡的数据传输 .....          | 136        |
| 任务3 电子钱包POS机终端控制软件设计与调试 .....  | 138        |
| 做一做 CPU卡读写软件设计与调试 .....        | 138        |
| 学一学 智能CPU卡的命令与操作程序 .....       | 144        |
| 4.3.1 CPU卡的通信协议与命令 .....       | 144        |
| 4.3.2 CPU卡的安全体系 .....          | 148        |
| 4.3.3 电子钱包卡操作程序 .....          | 150        |
| 拓展 智能卡安全技术 .....               | 153        |
| 拓展1 智能卡加密与认证技术 .....           | 153        |
| 拓展2 智能卡的攻击技术与安全设计策略 .....      | 158        |
| 思考题 .....                      | 163        |
| <b>第五章 射频识别(RFID)技术 .....</b>  | <b>164</b> |
| 引入 电子车牌识别系统需求分析 .....          | 164        |
| 任务1 电子车牌识别系统RFID标签选型 .....     | 165        |
| 做一做 RFID标签读写操作与特性测试 .....      | 166        |
| 学一学 RFID电子标签特性 .....           | 167        |
| 5.1.1 RFID电子标签的特性参数 .....      | 167        |
| 5.1.2 RFID电子标签的频谱特性 .....      | 170        |
| 5.1.3 标签封装基材与贴标材料特性 .....      | 172        |
| 5.1.4 RFID标签天线特性 .....         | 174        |
| 任务2 电子车牌识别系统搭建与阅读器设计 .....     | 176        |
| 做一做 UHF RFID阅读器硬件电路搭建与测试 ..... | 176        |
| 学一学 RFID系统硬件组成与读写器接口电路 .....   | 178        |

|                                  |            |
|----------------------------------|------------|
| 5.2.1 电子车牌识别系统硬件组成 .....         | 178        |
| 5.2.2 RFID 读写器接口电路设计 .....       | 180        |
| 5.2.3 RFID 读写器天线特性与安装调试 .....    | 182        |
| 任务3 电子车牌读写程序设计与测试 .....          | 185        |
| 做一做 RFID 标签读写程序调试与系统测试 .....     | 185        |
| 学一学 UHF RFID 通信协议与读写程序 .....     | 188        |
| 5.3.1 NXP UCODE 电子标签的存储结构 .....  | 188        |
| 5.3.2 EPCglobalGen2 标准通信协议 ..... | 190        |
| 5.3.3 RFID 电子标签读写程序设计 .....      | 194        |
| 5.3.4 RFID 应用系统测试 .....          | 200        |
| 拓展 RFID 标准与防冲突技术 .....           | 202        |
| 拓展1 EPC、RFID 与物联网 .....          | 202        |
| 拓展2 RFID 防冲突技术 .....             | 206        |
| 思考题 .....                        | 209        |
| <b>第六章 智能卡与 RFID 应用系统</b> .....  | <b>210</b> |
| 应用1 企业一卡通系统的系统集成 .....           | 210        |
| 6.1.1 企业一卡通系统需求分析 .....          | 210        |
| 6.1.2 企业一卡通系统的系统集成 .....         | 212        |
| 应用2 企业一卡通系统的应用维护 .....           | 221        |
| 综合训练1 设备卡片管理及考勤系统应用 .....        | 221        |
| 综合训练2 售饭管理系统应用 .....             | 227        |
| 综合训练3 门禁管理系统应用 .....             | 231        |
| 综合训练4 一卡通系统维护 .....              | 233        |
| 应用3 典型智能卡与 RFID 应用系统 .....       | 236        |
| 6.3.1 数字社区一卡通系统 .....            | 236        |
| 6.3.2 RFID 智能图书馆管理系统 .....       | 242        |
| 应用4 智能卡与 RFID 应用系统的开发方法 .....    | 248        |
| 思考题 .....                        | 255        |
| <b>参考文献</b> .....                | <b>256</b> |

# 第一章 智能卡技术入门

自 1976 年法国布尔(Bull)公司研制出世界首枚智能 IC 卡以来,智能卡技术飞速发展,已经形成一涉及全球众多著名电子巨头的新兴技术产业。同时,无线射频识别技术(RFID)作为本世纪最有发展前途的信息技术之一,也已得到全球业界的高度重视。国际标准化组织(ISO)与国际电工委员会(IEC)的联合技术委员会(JTC1)为之制定了一系列的国际标准、规范,极大地推动了智能卡与 RFID 的研究和发展。目前,智能卡与 RFID 技术的应用已遍布全球。

中国智能卡与 RFID 产业是伴随着国家金卡工程建设而形成的一个新兴产业,经过十多年的扎实发展,其应用已普及到诸多领域,银行卡 EMV 迁移、二代身份证换发、城市一卡通项目以及移动的酝酿等,是未来几年智能卡与 RFID 市场快速发展的动力,原有的应用领域如电信、校园、公交、社保及医疗保障等发卡量不断增长,与此同时,3G 网络及物联网建设、电子证照与商品防伪、供应链管理和现代物流管理、城市交通与安全管理、工业生产和安全管理以及特种设备强检等领域也都启动了应用试点。巨大的市场必将推动智能卡与 RFID 行业进入发展的“快车道”,也许明天,真的会一卡在手,天下全有。

本章旨在对智能卡与 RFID 技术的相关概念、技术要素、国际标准和应用概况加以粗略的描述,以使读者建立一个总体的概念,并大致了解智能卡与 RFID 系统的基本组成与工作过程。

## 基础 1 什么是智能卡

在当今这个信息时代,各种各样的卡在我们的日常生活中已随处可见,银行卡、乘车卡、学生卡、社保卡、电话卡、手机卡、加油卡、门禁卡、积分卡等不一而足,专业技术词汇则包括磁卡、条码卡、IC 卡、射频卡(RF Card)、微电路卡(Microcircuit Card)、微芯片卡(Microchip Card)等。那么,究竟什么是智能卡(Smart Card)?

### 1. 智能卡的概念

对于什么是智能卡,业界人士尚无统一、全面的定义,一般采用下述解释性描述:

智能卡即“集成电路卡”(ICC, Integrated Circuit Card),是将一个或多个集成电路芯片嵌装于塑料基片上制成的卡片,卡内的集成电路具有数据存储和运算、判断功能,并能与外部交换数据。符合 ISO ID1 定义的卡的外形尺寸是  $85.6\text{ mm} \times 53.98\text{ mm} \times 0.76\text{ mm}$ ,与银行所使用的磁卡相同,也可封装为射频标签、纽扣、钥匙、饰物等特殊形状,并也被统称为智能(IC)卡。

在智能卡推出之前,从世界范围来看,磁卡已得到广泛应用,为了从磁卡平稳过渡到智能卡,也是为了兼容,通常在智能卡上仍贴有磁条,为此,卡中封装集成电路芯片的位置受到磁条位置

的限制。图 1.1 为 IC 卡的外观图,正面中间的小方块中封装有集成电路芯片,其下面为签名条;最下面为凸印字符,用于压印账单;背面上部有磁条。正面还可印刷各种文字、图案、照片等。卡的尺寸、触点位置与用途、磁条的位置及数据格式等均有相应的国际标准予以明确规定。

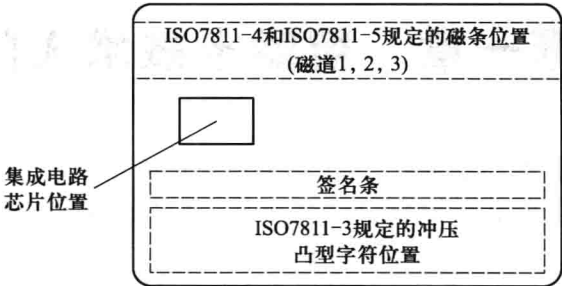


图 1.1 智能(IC)卡的外观

2. 智能卡的优势

磁卡的应用早于智能卡,并因其简单、低廉、使用方便,而在金融、邮电等领域得以广泛运用。但由于存储磁条外露且容量有限,在保密性、抗损性、可靠性及脱机工作等方面存在诸多不足。但由于美国等国已建立了基于磁卡的强大的授权通信网络,难以抛弃已有的大量设备资源,目前在金融领域仍主要采用磁卡。而欧洲各国如法国、芬兰等国的智能卡应用则比较普遍,技术水平也较为领先。然而,随着芯片技术的迅猛发展,智能卡凭借其突出的高安全性及应用灵活性优势,正逐步替代磁卡。

相对于磁卡,智能卡具有以下优点:

- ① 可靠性高:智能卡具有防磁、防静电、防机械损坏和防化学破坏等能力,信息一般可保存 100 年以上,擦写次数可达 10 万次以上。
  - ② 存储容量大:可存储文字、图像、声音等各种信息。
  - ③ 安全性高:物理层、硬件层、软件层三方面的安全策略,可以有效防止数据被非法修改或读取。
  - ④ 脱机应用:其安全性决定了对网络的实时性要求不高,可以脱机/非实时联机使用。
- 表 1.1 给出了磁卡与智能卡特性差异的对比。

表 1.1 智能卡与磁卡的比较

| 性 能   | 智 能 卡      | 磁 卡    |
|-------|------------|--------|
| 抗机械损伤 | 好          | 差      |
| 抗电磁干扰 | 是磁卡的 10 倍  | 差      |
| 抗静电   | 好          | 差      |
| 抗辐射   | 好          | 差      |
| 防潮防污  | 好          | 差      |
| 存储容量  | 已达 32 Mbit | 小于几百字节 |

续表

| 性 能     | 智 能 卡          | 磁 卡   |      |
|---------|----------------|-------|------|
| 数据保存期限  | 100 年          | 1~2 年 |      |
| 使用寿命    | 10 万次          | 几千次   |      |
| 卡的价格    | 较高             | 低     |      |
| 作业模式    | 脱机/非实时联机       | 脱机    | 实时联机 |
| 网络要求    | 较低             | 低     | 高    |
| 对主机的要求  | 较低             | 低     | 高    |
| 系统投资    | 中等             | 低     | 高    |
| 卡的复制与伪造 | 很难             | 容易    |      |
| 读写安全措施  | 读写保护、数据加密保护    | 无     |      |
| 使用保护    | 个人密码、卡与读写器双向认证 | 个人密码  |      |

### 3. 智能卡应用系统的构成

毫无疑问,智能卡本身并不能单独直接使用,它必须与相关设备组合,才能共同构成符合某种需求的应用系统。那么,一个完整的智能卡应用系统究竟包括哪些构成要素?可采取哪种结构模式呢?

一个标准智能卡应用系统的最基本构件为:智能卡、智能卡接口设备(智能卡读写器)、微机系统,较大的系统还包括通信网络和主计算机等,如图 1.2 所示。

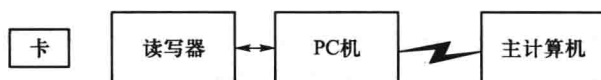


图 1.2 智能卡应用系统的基本硬件构成

#### (1) 智能卡(ICC, IC Card)

由持卡人掌管,记录有持卡人的特征代码、文件资料的便携式信息载体。

#### (2) 接口设备(IFD, InterFace Device)

即通常所说的 IC 卡读写器,是卡与 PC 机进行信息交换的桥梁,而且常常是 IC 卡的能量来源。其核心通常为工作可靠的工业控制单片机或嵌入式系统。IFD 与 IC 卡间遵循符合 ISO/IEC 国际标准的通信协议,通过自身的机械卡座或射频(RF)、红外等无线信道,以接触或非接触方式对卡读写,并通过 RS232/485 串行接口、USB 接口或以太网接口等以实时或非实时方式与 PC 机通信,实现卡与微机系统信息的上传下送。

#### (3) 微机系统

智能卡应用系统的核心,根据实际需求选用普通 PC 机或服务器,配有专用的智能卡应用系统管理软件,通常是基于数据库管理软件的信息管理系统,完成信息汇总、统计、计算、处理、报表生成输出和指令的发放、系统的监控管理以及卡的发行、挂失、黑名单的建立等。

#### (4) 网络

在金融服务等相对大的系统中,网络是使前端微机系统与上级控制/授权/服务/管理中心即中央电脑(主计算机)连接的必备条件。其借助通信线路、设备和完善的网络通信软件,将地理位置不同的各个子系统,有机相接为一功能完备的大系统;主计算机则是对此大系统实施监控管理的核心,是重大决策管理要素的源头。

综上所述,智能卡应用工程融微电子技术、嵌入式应用技术、数据库管理技术、网络技术、安全技术、射频识别技术以及数字印刷技术等多种高新技术于一身,是一个综合性的高新技术产业。

## 基础2 缤纷卡族

智能卡种类繁多,可以按不同形式分类。从应用的角度常分为金融卡和非金融卡,金融卡即银行卡如信用卡、借记卡、电子钱包(EP, Electronic Purse)卡等,非金融卡则涉及金融卡之外所有领域,诸如电信、社保、交通、教育等。而从技术的角度则多按卡内镶嵌的芯片或卡与读写器的接口方式来分类。

### 1.2.1 存储器卡与微处理器卡

按卡内镶嵌芯片的不同,可将智能卡分为存储器卡、逻辑加密卡 and 智能 CPU 卡(CPU 卡)三类。

#### 1. 存储器卡(Memory Card)

卡内嵌入的芯片为通用存储器芯片 EEPROM 或 Flash Memory;无安全控制逻辑,可对片内信息不受限制地任意存取;卡片制造中也很少采取安全保护措施;不完全符合或支持 ISO7816 国际协议,而多采用 2 线串行通信协议(I<sup>2</sup>C 总线协议)或 3 线串行通信协议。

存储器卡功能简单,没有或很少安全保护逻辑,但价格低廉、开发使用简便、存储容量增长迅猛,因此多用于某些简单的、内部信息无需保密或不允许加密(如急救卡)的场合。

#### 2. 逻辑加密卡(Security Card)

也称为加密存储器卡(Security Memory Card),由非易失性存储器和硬件加密逻辑构成,一般均为专门为 IC 卡设计的芯片,具有安全控制逻辑,安全性能较好;同时采用 ROM、PROM、EEPROM 等存储技术;从芯片制造到交货,均采取较好安全保护措施,如运输密码 TC(Transport Card)的取用;支持 ISO7816 国际协议。

逻辑加密卡有一定的安全保证,多用于有一定安全要求的场合,如保险卡、加油卡、驾驶卡、借书卡、IC 卡电话、小额电子钱包等。

#### 3. 智能 CPU 卡(CPU Card)

智能 CPU 卡(简称 CPU 卡)也称芯片卡、微处理器卡,在 IC 卡家族中出现最晚、也最具生命

力。CPU 卡具有微型计算机软硬件配置,其硬件构成包括:CPU、存储器(含 RAM、ROM、EEPROM 等)、卡与读写终端通信的 I/O 接口及用于信息安全保护的加密协处理器、随机数发生器及物理攻击自毁电路,ROM 中则装载有系统软件——片内操作系统 COS。

由于 CPU 卡具有很高的数据处理和计算能力、较大存储容量以及开放式的应用设计平台,因此应用的灵活性、适应性较强;而在硬件结构、操作系统、制作工艺上所取之多层次安全措施,则保证了其极强的安全防伪能力。它不仅可验证卡和持卡人的合法性,而且可鉴别读写终端,已成为一卡多用及对数据安全保密性特别敏感场合的最佳选择,如金融信用卡、手机 SIM 卡、社保卡、电子护照等。

虽然通常将所有 IC 卡都称作智能卡,但严格地讲,存储器卡与逻辑加密卡都只具备数据存储功能,只有 CPU 卡才真正具有智能特征,也即只有 CPU 卡才是真正意义上的“智能卡”。

### 1.2.2 接触式与非接触式 IC 卡

根据卡与外界数据交换界面的不同分为接触式 IC 卡和非接触式 IC 卡。接触式 IC 卡通过卡表面的多个金属触点实现与读写机具的信息和能量传递,成本低,实施相对简便;非接触式 IC 卡则不用触点,而是在卡中敷设天线,借助无线收发传送信息,因此在前者难以胜任的交通、门禁等诸多场合有较多应用。此外,还有兼备接触式和非接触式两种接口的双介面卡。

#### 1. 接触式 IC 卡(Contact ICC)

所谓接触式 IC 卡就是在使用时,通过有形的金属电极触点将卡的集成电路与外部接口设备直接接触连接,提供集成电路工作的电源并进行数据交换的 IC 卡。接触式 IC 卡由半导体芯片、电极模片(卡触点)、塑料基片组成,其特点是在卡的表面有符合 ISO7816 标准的多个金属触点,如图 1.3 所示。

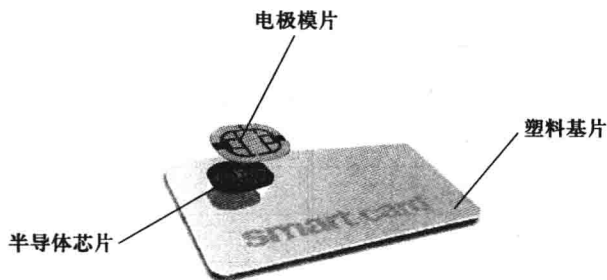


图 1.3 接触式 IC 卡结构图

##### (1) 半导体芯片

它是 IC 卡的核心部分。一般采用  $0.8\mu\text{m}$  至  $0.35\mu\text{m}$  的 CMOS 或 BiCMOS 工艺制造的超大规模集成电路,随着半导体工艺的进步,目前已更多采用  $0.6\mu\text{m}$ 、 $0.25\mu\text{m}$  以至  $0.13\mu\text{m}$  嵌入式存储器工艺设计制造智能 CPU 卡芯片。在 IC 卡半导体芯片中集成了存储器、译码电路、接口驱动电路、逻辑加密控制电路、微处理器单元(CPU)等各种功能电路,其外形大小约为:  $2\text{mm} \times 1\text{mm} \times 0.3\text{mm}$ 。

##### (2) 电极模片

通常被称为“触点”,是半导体芯片各输入输出信号引脚与外部设备接触连接的导体。它实际是一种精密的印制电路板(PCB),其基底为一层绝缘材料,(一般为环氧树脂玻璃或聚酰亚胺薄膜),在其上沉积一层铜合金,并在其外端表面镀金,以提高其导电性能和防氧化能力。电极模片的外形大小约为:长 $9.62 \sim 13.65 \text{ mm}$ ,宽 $9.32 \sim 11.56 \text{ mm}$ ,形状一般为矩形或椭圆形。这种形状上的差异主要是为了改善卡片在抗扭曲方面的机械特性。

接触式 IC 卡有 8 个触点,即集成电路引脚,从 C1 到 C8,如图 1.4 所示,IC 卡的触点之间的排列顺序、尺寸及位置必须符合由国际标准 ISO/IEC7816-2 的规定,每个触点的功能定义见表 1.2。

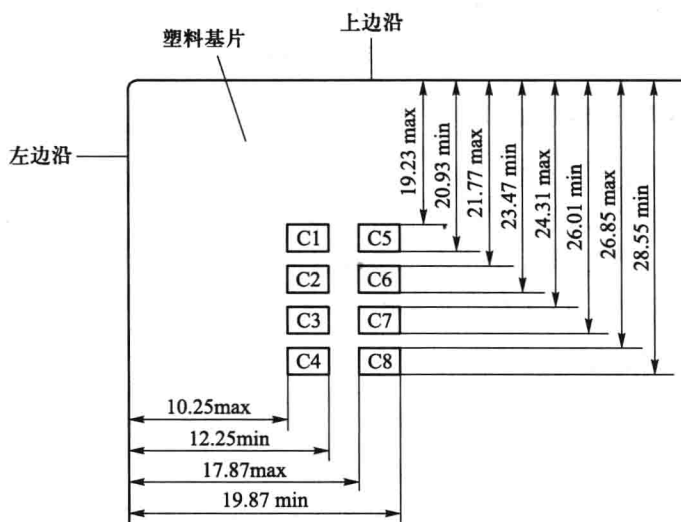


图 1.4 接触式 IC 卡的触点位置

表 1.2 接触式 IC 卡的触点功能

| 触点编号 | 功 能                       | 触点编号 | 功 能                       |
|------|---------------------------|------|---------------------------|
| C1   | $V_{cc}$ (电源电压)           | C5   | GND (地)                   |
| C2   | RST (复位信号)                | C6   | $V_{pp}$ (编程电压)           |
| C3   | CLK (时钟)                  | C7   | I/O (数据输入/输出端)            |
| C4   | ISO/IEC JTC1/SC1T<br>保留使用 | C8   | ISO/IEC JTC1/SC17<br>保留使用 |

通常,半导体厂商提供给制卡商的是半导体芯片和电极模片封装而成的 IC 卡模块(Wire Boded Module)。

### (3) 塑料基片

它是半导体芯片和电极模片的载体。根据各生产厂家制卡工艺设备的要求,一般采用 PVC, PET 和 ABS 塑料材料。塑料基片的大小,对于满足国际标准——识别卡的 ID-1 型的尺寸是:  $85.6$  (宽)  $\text{mm} \times 53.98$  (高)  $\text{mm} \times 0.75$  (厚)  $\text{mm}$ , 卡生产厂商在基片上冲孔、填入封装树脂并通过热压将 IC 卡模块嵌入其中,即制成一张接触式 IC 卡。

## 2. 非接触式 IC 卡 (Contactless ICC)

非接触式 IC 卡是在卡中敷设天线,卡芯片利用天线的接收发射与读写器的天线交换信号,实现一种无线通信,非接触式 IC 卡的基本结构如图 1.5 所示,它是卡技术与射频技术的结合,因此,非接触式 IC 卡又被称为射频卡(RFC, Radio Frequency Card),简称 RF 卡,非接触式 IC 卡系统是射频识别系统(RFID, Radio Frequency Identification)的一种。

非接触式 IC 卡中嵌有耦合元件(天线线圈)和集成电路芯片。通常,非接触式 IC 卡没有自己的供电电源(电池),当卡处于读写器响应范围内时,卡所需要的能量、时钟脉冲及数据,均通过耦合单元的电磁耦合作用传输给卡。

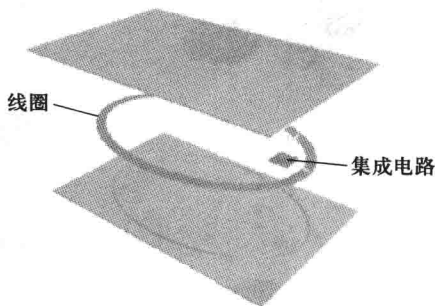


图 1.5 非接触式 IC 卡的基本结构

非接触式 IC 卡的外形尺寸符合国际标准 ISO7810 对 ID-1 型卡的规定(85.72 mm × 54.03 mm × 0.76 mm),其制造工艺是在四层 PVC 薄膜(两层嵌入薄膜和两层覆盖薄膜)之间粘合一个非接触式 IC 卡模块及耦合元件而构成的,其中,耦合元件一般为电磁感应天线线圈,起电感耦合作用。将设计成线圈状的天线安放在承载薄膜的上面,且用适当的连接技术将其与芯片模块连接在一起。天线的制造主要采用以下四种方法:绕制工艺、布线工艺、丝网印刷工艺和蚀刻工艺。

在 1.2.1 节中已经提到,按照嵌入芯片的不同,可将 IC 卡分类作存储器卡、逻辑加密卡和 CPU 卡。这种分类对接触式和非接触式 IC 卡均适用。

### 1.2.3 RFID 电子标签

RFID(Radio Frequency Identification)即射频识别,是一种非接触式的自动识别技术,它通过无线射频信号的空间耦合(感应或散射)自动识别目标对象并获取相关数据。

最基本的 RFID 系统由标签(Tag)、阅读器(Reader)和天线(Antenna)组成,如图 1.6 所示。

- RFID 标签:由耦合元件(天线)及芯片组成,每个标签具有唯一的电子编码,附着在物体上标识目标对象;根据应用需求,RFID 标签可以封装成柔性贴纸、塑料卡片、钥匙扣、手表、动物耳标、托盘等多种形式,如图 1.7 所示。

- 阅读器(Reader):读取(有时还可以写入)标签信息的设备,可设计为手持式或固定式。

- 天线:在标签和读取器间传递射频信号。

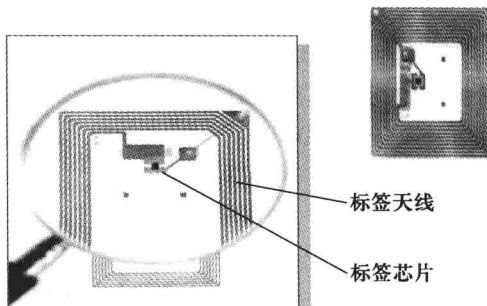


图 1.6 RFID 标签的构成

RFID 系统在实际应用中是将电子标签附着在待识别物体的表面,电子标签中保存有约定格式的电子数据,阅读器通过天线发送出一定频率的射频信号,当标签进入磁场时产生感应电流从而获得能量,发送出存储在芯片中的产品信息(Passive Tag,无源标签或被动标签),或者由标签主动发送某一频率的信号(Active Tag,有源标签或主动标签),阅读器读取信息并译码后,送至中央信息系统进行有关数据处理,如图 1.8 所示。

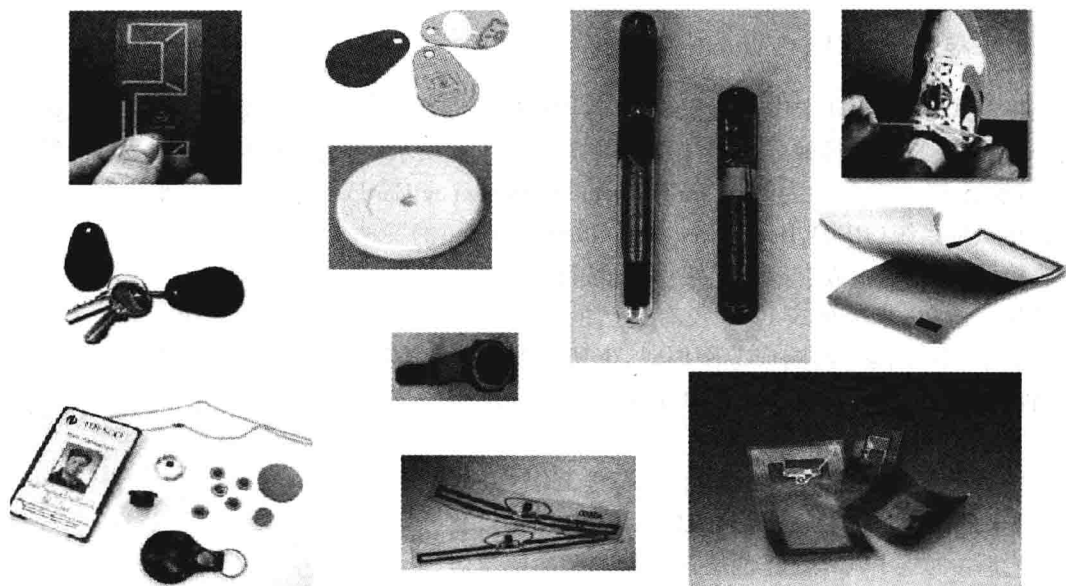


图 1.7 RFID 标签的封装形式

## 3. 识读器采集信息并译码

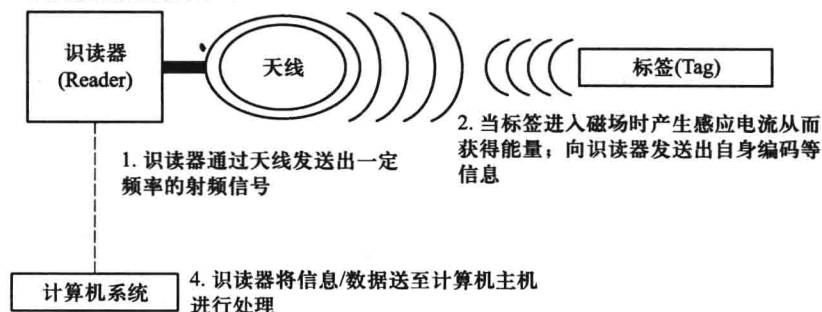


图 1.8 RFID 系统构成

由以上对 RFID 系统的基本描述可以看出,RFID 标签的构成与非接触式 IC 卡完全一致,只是封装基材及对应的制造工艺不同,因此,非接触式 IC 卡即是 RFID 电子标签的一种,常被称为 RF 卡。关于 RFID 标签、阅读器和天线的应用技术、RFID 系统集成方式以及 RFID 相关标准的详细内容参见第三章、第五章和第六章。

## 基础 3 智能卡的用卡过程与优势

### 1.3.1 智能卡的设计制造和应用过程

智能卡从最初的设计到最后失效,一般要经过 5 个阶段:设计、制造、发行、使用和回收。

## 1. 设计阶段

### (1) 系统设计

根据应用系统对卡功能和安全的 yêu cầu设计卡内芯片(或考虑设计通用芯片),并根据工艺水平和成本对智能卡的 MPU、存储器容量和 COS 提出具体要求,或对逻辑加密卡的逻辑功能和存储区的分配提出具体要求。

### (2) 卡内集成电路设计

其设计过程与 ASIC(专用集成电路)的设计类似,包括逻辑设计、逻辑模拟、电路设计、电路模拟、版图设计和正确性验证等。对于智能卡,经常采用工业标准微处理器作为核心,调整存储器的种类和容量,而不必重新设计。为可靠起见,这些芯片应该有自保护能力。例如,当外加电压不正常时(高低电压检测),芯片应停止工作,时钟频率超出正常范围时也应相应的措施。

### (3) 软件设计

包括 COS 和应用软件的设计,有相应的开发工具可供选用。由于智能卡的安全性与 COS 有关,因此在国家重要经济部门和机密部门使用的智能卡,应写入具有自主知识产权的 COS。

## 2. 制造阶段

### (1) 芯片制造

- 在单晶硅圆片(Wafer)上制作电路。

设计者将设计好的版图或 COS 代码提交给芯片制造厂。制造厂根据设计与工艺过程的要求,产生多层掩膜版。在一个圆片上可制作几百~几千个相互独立的电路,每个电路即为一个芯片(die)。对于接触式 IC 卡,小片上除有按 IC 卡标准(8 个触点)设计的压焊块外,还应有专供测试用的探针压块,但要注意这些压块是否会给攻击者以可乘之机。

- 测试并在 EEPROM 中写入信息。

利用带测试程序的计算机控制探头测试圆片上的每个芯片。在有缺陷的芯片上做标记,在测试合格的芯片中写入厂商代码及传输密码等信息。

- 研磨和切割圆片。

厚度要符合 IC 卡的规定,研磨后将圆片切割成众多小芯片。

### (2) 微模块制造

将制造好的芯片安装在有 8 个触点的印制电路薄片上,称作微模块。

### (3) 卡片制造

完成卡片表面的印刷工作,并将微模块嵌入卡片中。

## 3. 发行阶段

### (1) 卡初始化

发行商从制造商手中取得卡片后,先核对传输密码。如为逻辑加密卡,传输密码由制造厂写入用户密码区,发行商核对正确后改写成用户密码;对于智能卡,在此时可进行写入密码、密钥、建立文件等操作。