物联网工程专业系列教材

物联网应用
综合项目开发

主　编　陈　广
副主编　王子玉　陈胜华　伍德鹏　伍德雁

中国水利水电出版社
www.waterpub.com.cn

物联网工程专业系列教材

物联网应用综合项目开发

主　编　陈　广

副主编　王子玉　陈胜华　伍德鹏　伍德雁

中国水利水电出版社
www.waterpub.com.cn

内 容 提 要

本书分为两部分，第一部分为理论部分，首先介绍了RFID射频技术和无线传感网的相关知识，然后介绍了北京京胜世纪科技有限公司开发的物联网虚拟仿真实验平台的使用方法，最后通过一个图书管理系统实例让学生了解和掌握综合应用系统的开发；第二部分为实训指导部分，通过开发一个超市管理系统，让学生有效整合之前所学知识。

本书非常适合作为高职高专物联网专业及相关专业的教材，同时也适合作为自学教材以及物联网开发人员的参考书。

图书在版编目（CIP）数据

物联网应用综合项目开发 / 陈广主编. -- 北京 : 中国水利水电出版社, 2016.6（2017.9重印）
物联网工程专业系列教材
ISBN 978-7-5170-4466-6

Ⅰ. ①物… Ⅱ. ①陈… Ⅲ. ①互联网络－应用－高等职业教育－教材②智能技术－应用－高等职业教育－教材
Ⅳ. ①TP393.4②TP18

中国版本图书馆CIP数据核字(2016)第142177号

策划编辑：石永峰　责任编辑：李　炎　加工编辑：郭继琼　封面设计：李　佳

书　名	物联网工程专业系列教材 **物联网应用综合项目开发**
作　者	主　编　陈　广 副主编　王子玉　陈胜华　伍德鹏　伍德雁
出版发行	中国水利水电出版社 （北京市海淀区玉渊潭南路1号D座　100038） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）68367658（发行部）、82562819（万水）
经　售	北京科水图书销售中心（零售） 电话：（010）88383994、63202643、68545874 全国各地新华书店和相关出版物销售网点
排　版	北京万水电子信息有限公司
印　刷	三河市铭浩彩色印装有限公司
规　格	184mm×260mm　16开本　12印张　295千字
版　次	2016年6月第1版　2017年9月第2次印刷
定　价	28.00元

凡购买我社图书，如有缺页、倒页、脱页的，本社发行部负责调换

前　言

互联网已渐渐成为人们日常生活的信息载体和平台，并广泛参与到社会的运行和人们的各种活动中。而国民经济的发展对信息系统也提出了更高的要求，并要求将计算机技术拓展到整个人类生存和活动的空间中，将人类的物理世界网络化、信息化，实现物理世界和信息系统的整合统一。在这种意义上来说，下一代互联网将是物联化的互联网。

本书通过讲述两个物联网应用综合实例——图书管理系统和智慧超市管理系统，让学生理解和掌握物联网技术在现实生活中的应用，并让学生把之前所学的无线传感器网知识、RFID 无线射频知识、C#程序设计知识、数据库知识和软件工程知识有效地整合在一起进行综合应用。

为了方便学生进行实验，本书使用了北京京胜世纪科技有限公司开发的物联网虚拟仿真实验平台作为开发平台，所有实验效果均可以在该虚拟平台中看到。本书也对该平台的使用及其使用的网络协议进行了详细的介绍。

本书由广西机电职业技术学院和北京京胜世纪科技有限公司共同编写完成，属校企共建教材。

本书的先导课程有“C#程序设计”“数据库 SQL Server”“无线传感器网络技术”“RFID 技术”“软件工程”。

本书非常适合作为高职高专物联网专业及相关专业的教材，同时也适合作为自学教材以及物联网开发人员的参考书。

编　者

2016 年 3 月

目　录

前言

第一部分　理论部分

第 1 章　RFID 综合概述 …… 1
1.1　RFID 技术发展现状综述 …… 1
1.2　RFID 原理及简介 …… 2
1.2.1　RFID 原理 …… 2
1.2.2　RFID 组成 …… 2
1.2.3　RFID 工作原理 …… 3
1.2.4　RFID 标准及分类 …… 4
1.3　ISO14443 …… 5
1.3.1　ISO14443 协议 …… 5
1.3.2　Mifare S50 与 Mifare S70 原理 …… 7
1.3.3　Mifare S50 与 Mifare S70 的存取控制 …… 10
1.4　ISO15693 …… 13
1.4.1　ISO15693 的载波、调制与编码 …… 13
1.4.2　ISO15693 的防冲突与传输协议 …… 15
第 2 章　无线传感器网络 …… 17
2.1　无线传感器网络概述 …… 17
2.2　无线传感器网络的体系结构 …… 17
2.3　无线传感器网络的特征 …… 18
2.4　无线传感器网络中的关键技术 …… 19
2.5　无线传感器网络的安全需求 …… 20
2.6　无线传感器网络的主要用途 …… 20
2.7　无线传感器网络的拓扑维护 …… 22
2.7.1　拓扑维护基础 …… 22
2.7.2　拓扑维护模型 …… 23
第 3 章　物联网教学系统操作简介 …… 24
3.1　RFID 教学实验系统硬件平台简介 …… 24
3.2　物联网虚拟仿真实验平台简介 …… 25
3.2.1　平台简介 …… 25
3.2.2　运行环境 …… 25
3.2.3　功能说明 …… 25
第 4 章　ISO14443 读写操作 …… 35
4.1　ISO14443 的 API 参考手册 …… 35
4.2　ISO14443 的读写示例 …… 37
第 5 章　无线传感器网络的访问控制 …… 45
5.1　WSN 动态链接库使用方法及注意事项 … 45
5.2　WSN 动态链接库函数接口 …… 46
5.2.1　总体描述 …… 46
5.2.2　函数列表 …… 49
5.2.3　函数详细说明 …… 50
5.3　无线传感器网络的访问控制实例 …… 56
第 6 章　图书管理系统需求分析及数据库设计 … 62
6.1　任务概述 …… 62
6.1.1　项目背景 …… 62
6.1.2　任务概述 …… 62
6.1.3　需求概述 …… 62
6.1.4　功能层次图 …… 63
6.2　数据描述 …… 63
6.2.1　静态数据 …… 63
6.2.2　动态数据 …… 64
6.2.3　数据流图与数据字典 …… 64
6.2.4　数据关系 E-R 图 …… 68
6.3　功能需求 …… 69
6.3.1　功能划分 …… 69
6.3.2　功能描述 …… 69
6.4　性能需求 …… 69
6.5　运行需求 …… 70
6.6　数据库设计 …… 70
6.6.1　数据库视图 …… 70
6.6.2　建表 SQL 语句 …… 70

第 7 章　图书管理系统程序设计 …… 72
7.1　用户登录模块设计 …… 72
7.1.1　登录窗体界面设计 …… 72
7.1.2　登录窗体代码设计 …… 72
7.1.3　用户信息窗体界面设计 …… 74
7.1.4　用户信息窗体代码设计 …… 74
7.1.5　用户列表窗体界面设计 …… 79
7.1.6　用户列表窗体代码设计 …… 79
7.2　图书信息模块设计 …… 82
7.2.1　图书上架窗体界面设计 …… 82
7.2.2　图书上架窗体代码设计 …… 82
7.2.3　图书信息窗体界面设计 …… 86
7.2.4　图书信息窗体代码设计 …… 86
7.3　图书借阅卡管理模块设计 …… 89
7.3.1　借阅卡信息窗体界面设计 …… 89
7.3.2　借阅卡信息窗体代码设计 …… 90
7.3.3　借阅卡管理窗体界面设计 …… 93
7.3.4　借阅卡管理窗体代码设计 …… 93
7.4　借书模块设计 …… 98
7.4.1　借书窗体界面设计 …… 98
7.4.2　借书窗体代码设计 …… 99
7.5　还书模块设计 …… 102
7.5.1　还书窗体界面设计 …… 102
7.5.2　还书窗体代码设计 …… 102

第二部分　实训指导

第 8 章　智慧超市需求分析 …… 105
8.1　立项背景 …… 105
8.2　项目概述 …… 105
8.2.1　面向的用户 …… 105
8.2.2　实现目标 …… 105
8.2.3　项目开发要求 …… 105
8.2.4　开发工具 …… 106
8.3　系统描述 …… 106
8.3.1　系统概述 …… 106
8.3.2　系统总体结构 …… 106
8.3.3　各部分功能描述 …… 106
8.4　系统分析 …… 107
8.4.1　用例图 …… 107
8.4.2　活动框图 …… 119
8.4.3　时序图 …… 124
8.4.4　类分析 …… 127
8.4.5　类设计 …… 130
8.4.6　库存管理信息系统部署图 …… 131
第 9 章　数据库设计 …… 132
9.1　数据库视图 …… 132
9.2　建表 SQL 语句 …… 132
第 10 章　主窗体及登录模块 …… 138
10.1　主窗体设计 …… 138
10.1.1　主窗体界面设计 …… 138
10.1.2　主窗体代码设计 …… 138
10.2　主窗体设计 …… 143
10.2.1　登录窗体界面设计 …… 143
10.2.2　登录窗体代码设计 …… 144
第 11 章　系统管理模块 …… 146
11.1　添加用户窗体设计 …… 146
11.1.1　添加用户窗体界面设计 …… 146
11.1.2　添加用户窗体代码设计 …… 146
11.2　用户管理窗体设计 …… 150
11.2.1　用户管理窗体界面设计 …… 150
11.2.2　用户管理窗体代码设计 …… 151
11.3　修改密码窗体设计 …… 154
11.3.1　修改密码窗体界面设计 …… 154
11.3.2　修改密码窗体代码设计 …… 154
第 12 章　商品管理模块 …… 156
12.1　商品管理窗体设计 …… 156
12.1.1　商品管理窗体界面设计 …… 156
12.1.2　商品管理窗体代码设计 …… 156
12.2　商品分类管理窗体设计 …… 161
12.2.1　商品分类管理窗体界面设计 …… 161
12.2.2　商品分类管理窗体代码设计 …… 161
12.3　商品分类管理窗体设计 …… 164
12.3.1　商品分类管理窗体界面设计 …… 164
12.3.2　商品分类管理窗体代码设计 …… 164

12.4 商品分类管理窗体设计 …… 166
12.4.1 商品分类管理窗体界面设计…… 166
12.4.2 商品分类管理窗体代码设计…… 167
第 13 章 上架管理模块…… 172
13.1 上架管理窗体设计 …… 172
13.1.1 上架管理窗体界面设计…… 172
13.1.2 上架管理窗体代码设计…… 172
13.2 上架商品明细窗体设计 …… 177
13.2.1 上架商品明细窗体界面设计…… 177
13.2.2 上架商品明细窗体代码设计 …… 177
第 14 章 统计模块 …… 179
14.1 销售统计设计 …… 179
14.1.1 销售统计窗体界面设计 …… 179
14.1.2 销售统计窗体代码设计 …… 179
14.2 库存统计设计 …… 182
14.2.1 库存统计窗体界面设计 …… 182
14.2.2 库存统计窗体代码设计 …… 182

第一部分　理论部分

第 1 章　RFID 综合概述

1.1　RFID 技术发展现状综述

近几年来 RFID 技术发展迅猛，其应用领域也越来越广泛。而物联网行业的飞速发展，也不断地推动着 RFID 技术层面上的革新，各种 RFID 设备在物联网中得到充分应用。由于具有高速移动物体识别、多目标识别和非接触识别等特点，RFID 技术在管理、生产、信息传输等方面显示出巨大的发展潜力与应用空间，被认为是 21 世纪最有发展前途的信息技术之一。

RFID 技术涉及信息、制造、材料等诸多高技术领域，涵盖无线通信、芯片设计与制造、天线设计与制造、标签封装、系统集成、信息安全等技术。各国都在加速推动 RFID 技术的研发和应用进程。在过去的十年间，共产生数千项关于 RFID 技术的专利，主要集中在美国、欧洲、日本等国家。

按照能量供给方式的不同，RFID 标签分为有源、无源和半有源三种；按照工作频率的不同，RFID 标签分为低频（LF）、高频（HF）、超高频（UHF）和微波频段（MW）四种。目前国际上 RFID 的应用以 LF 和 HF 标签产品为主；UHF 标签也开始规模生产，由于其具有可远距离识别和低成本的优势，有望在未来五年内成为主流；MW 标签在部分国家已经得到应用。我国已掌握 HF 芯片的设计技术，并且成功地实现了产业化，同时 UHF 芯片也已经完成开发。

1. RFID 天线的应用

目前 RFID 标签天线制造以蚀刻/冲压为主，其材料一般为铝或铜，随着新型导电油墨的开发，印刷天线的优势将越来越突出。RFID 标签封装以低温倒装键合工艺为主，目前市场上也出现了流体自装配、振动装配等新的标签封装工艺。我国低成本、高可靠性的标签制造装备和封装工艺正在研发中。

2. RFID 读写器的应用

RFID 读写器产品类型较多，部分先进产品可以实现多协议兼容。我国已经推出了系列 RFID 读写器产品，小功率读写模块已达到国外同类水平，大功率读写模块和读写器片上系统（SoC）尚处于研发阶段。

3. RFID 的应用方向

在应用系统集成和数据管理等方面，某些国际组织提出基于 RFID 的应用体系架构。各大软件厂商也在其产品中提供了支持 RFID 的服务及解决方案，相关的测试和应用推广工作正在进行中。我国在 RFID 应用架构、公共服务体系、中间件、系统集成以及信息融合和测试工作等方面取得了初步成果，建立国家 RFID 测试中心已经被列入科技发展规划。

我国已经将 RFID 技术应用于铁路车号识别、身份证和票证管理、动物标识、特种设备与

危险品管理、公共交通管理以及生产过程管理等多个领域。

1.2 RFID 原理及简介

RFID 技术就是无线射频识别技术，是一种结合多门学科、多类技术的应用技术，目前应用最广泛的是在电子标签行业。相对于传统的磁卡及 IC 卡技术，RFID 技术具有非接触、阅读速度快、无磨损等特点，因此，在近几年里得到快速发展。为加强工程师对该技术的理解，本节详细介绍了 RFID 技术的结构、分类、标准以及工作原理等。

1.2.1 RFID原理

RFID 射频识别技术是一种非接触式的自动识别技术，其基本原理是电磁理论。它通过射频信号自动识别目标对象并获取相关数据，识别工作无须人工干预，可工作于各种恶劣环境中。RFID 技术可识别高速运动的物体并可同时识别多个标签，操作快捷方便。

埃森哲实验室首席科学家弗格森认为 RFID 是一种突破性的技术："第一，可以识别单个的、非常具体的物体，而不像条形码那样只能识别一类物体；第二，其采用无线电射频，可以透过外部材料读取数据，而条形码必须靠激光来读取信息；第三，可以同时对多个物体进行识读，而条形码只能一个一个地读，此外，RFID 存储的信息量也非常大。"

1.2.2 RFID 组成

最基本的 RFID 系统由电子标签、阅读器和计算机网络三部分组成。

（1）电子标签（tag）：电子标签包含电子芯片和天线，天线在标签和阅读器之间传递射频信号，电子芯片用来存储物体的数据，天线用来收发无线电波。

电子标签按供电方式分为无源电子标签、有源电子标签和半有源电子标签三种。

- 无源电子标签：标签内部没有电池，其工作能量均需阅读器发射的电磁场来提供，重量轻、体积小、寿命长、成本低，可制成各种卡片，是目前最流行的电子标签；但其识别距离比有源系统要小，一般为几米到十几米，而且需要较大的阅读器发射功率。无源电子标签如图 1.1 所示。

图 1.1 无源电子标签

- 有源电子标签：通过标签内部的电池来供电，不需要阅读器提供能量来启动，标签可主动发射电磁信号，识别距离较长，通常可达几十米甚至上百米；缺点是成本高、寿命有限，而且不易做成薄卡。有源电子标签如图 1.2 所示。

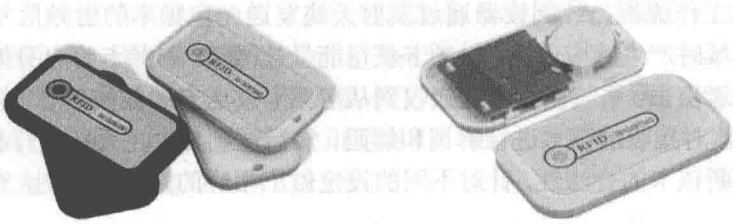

图 1.2 有源电子标签

- 半有源电子标签：内有电池，但电池只对标签内部电路供电，并不主动发射信号，其能量传递方式与无源系统类似，因此工作寿命比一般有源系统标签要长许多。

（2）阅读器（reader）：利用射频技术读写电子标签的设备，接收电子标签的数据信息，并将其传送给外部主机，如图 1.3 所示。

图 1.3 阅读器

（3）计算机网络（computer network）：阅读器通过标准接口与计算机网络连接，计算机网络完成数据的处理、传输和通信的功能。

1.2.3 RFID工作原理

射频识别系统的基本工作流程如图 1.4 所示。其中，电子标签又称为射频标签、应答器、数据载体；阅读器又称为读出装置，扫描器、通信器、读写器（取决于电子标签是否可以无线改写数据）。电子标签与阅读器之间通过耦合元件实现射频信号的空间（无接触）耦合，在耦合通道内，根据时序关系，实现能量的传递、数据的交换。

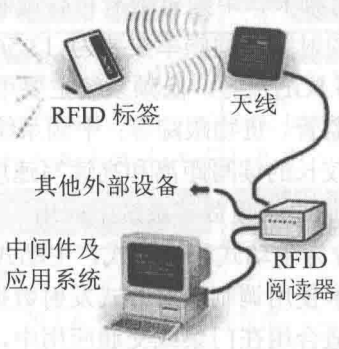

图 1.4 RFID 基本工作流程

系统的基本工作流程是：阅读器通过发射天线发送一定频率的射频信号，当射频卡进入发射天线工作区域时产生感应电流，射频卡获得能量被激活；射频卡将自身编码等信息通过卡内置发送天线发送出去；系统接收天线接收到从射频卡发送来的载波信号，经天线调节器传送到阅读器，阅读器对接收的信号进行解调和解码，然后送到后台主系统进行相关处理；主系统根据逻辑运算判断该卡的合法性，针对不同的设定做出相应的处理和控制，发出指令信号控制执行机构动作。

发生在阅读器和电子标签之间的射频信号的耦合类型有两种。

（1）电感耦合。变压器模型，通过空间高频交变磁场实现耦合，依据的是电磁感应定律，如图1.5所示。电感耦合方式一般适用于中、低频工作的近距离射频识别系统。典型的工作频率有：125kHz、225kHz和13.56MHz。识别作用距离小于1m，典型作用距离为10～20cm。

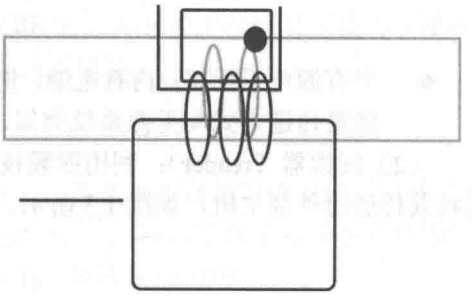

图1.5　电感耦合

（2）电磁反向散射耦合。雷达原理模型，发射出去的电磁波碰到目标后反射，同时携带回目标信息，依据的是电磁波的空间传播规律。电磁反向散射耦合方式一般适用于高频、微波工作的远距离射频识别系统。典型的工作频率有：433MHz、915MHz、2.45GHz、5.8GHz。识别作用距离大于1m，典型作用距离为3～10m。

1.2.4　RFID标准及分类

生产RFID产品的很多公司都采用自己的标准，因此，国际上还没有统一的标准。目前，可供射频卡使用的标准有：ISO10536、ISO14443、ISO15693和ISO18000。应用最多的是ISO14443和ISO15693，这两个标准都由物理特性、射频功率和信号接口、初始化和反碰撞，以及传输协议四部分组成。

按照不同的方式，射频卡有以下几种分类：

（1）按供电方式分为有源卡和无源卡。有源卡是指卡内有电池提供电源，其作用距离较远，但寿命有限、体积较大、成本高，且不适合在恶劣环境下工作；无源卡内无电池，它利用波束供电技术将接收到的射频能量转化为直流电源为卡内电路供电，其作用距离相对有源卡短，但寿命长且对工作环境的要求不高。

（2）按载波频率分为低频射频卡、中频射频卡和高频射频卡。低频射频卡的频率主要有125kHz和134.2kHz两种，中频射频卡的频率主要为13.56MHz，高频射频卡的频率主要为433MHz、915MHz、2.45GHz、5.8GHz等。低频系统主要用于短距离、低成本的应用中，如多数的门禁控制、校园卡、动物监管、货物跟踪等；中频系统用于门禁控制和需传送大量数据的应用系统；高频系统用于需要较长的读写距离和高读写速度的场合，其天线波束方向较窄且价格较高，主要在火车监控、高速公路收费等系统中应用。

（3）按调制方式的不同可分为主动式和被动式。主动式射频卡用自身的射频能量主动地发送数据给阅读器；被动式射频卡使用调制散射方式发射数据，它必须利用阅读器的载波来调制自己的信号，被动式调制技术适合用在门禁或交通应用中，因为阅读器可以确保只激活一定范围之内的射频卡。在有障碍物的情况下，使用调制散射方式，阅读器的能量必须来回穿过障

碍物两次，而主动方式的射频卡发射的信号仅穿过障碍物一次，因此主动方式工作的射频卡主要用于有障碍物的应用中，作用距离更远（可达 30m）。

（4）按作用距离可分为密耦合卡（作用距离小于 1cm）、近耦合卡（作用距离小于 15cm）、疏耦合卡（作用距离约 1m）和远耦合卡（作用距离 1～10m，甚至更远）。

（5）按芯片分为只读卡、读写卡和 CPU 卡。

1.3 ISO14443

非接触 IC 卡又称射频卡，是射频识别技术和 IC 卡技术有机结合的产物。它解决了无源（卡中无电源）和免接触这两大难题，具有更加方便、快捷的特点，广泛用于电子支付、通道控制、公交收费、停车收费、食堂售饭、考勤和门禁等多种场合。

非接触 IC 卡与条码卡、磁卡、接触式 IC 卡相比，具有高安全性、高可靠性、使用方便快捷等特点，这主要是由其技术特点决定的，在近距离耦合应用中主要遵循的标准是 ISO/IEC14443。

1.3.1 ISO14443 协议

ISO14443 分为四部分，硬件主要需要了解前两部分，软件和应用开发则需要了解后两部分，即 ISO14443-3 和 ISO14443-4。

ISO14443-1 定义了 IC 卡的物理特性。

ISO14443-2 定义了频率、射频能量、编码等内容。

ISO14443-3 定义了 TypeA/TypeB 的初始化和防冲突机制。

ISO14443-4 定义了卡片的数据传输协议。

ISO14443-2 定义了 NFC 的频率为 13.56MHz±7kHz，定义了最大和最小的能量场的范围值以及 TypeA、TypeB 的调制方式，如图 1.6 所示。

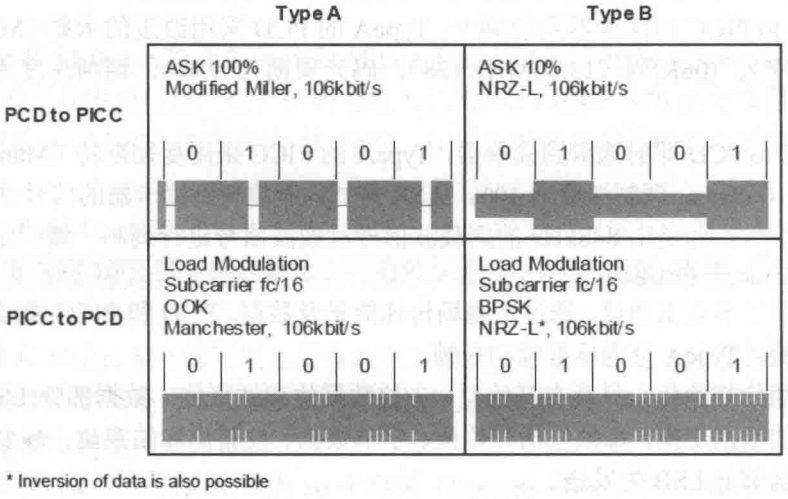

图 1.6 NFC 的调制方式

对比可以看出 TypeA 的 PCD 采用了 100% 的调制方式，而 TypeB 则采用了 10% 的调

制方式，TypeA 能量传送并不均匀，而 TypeB 采用的 10%ASK 方式对于射频卡来说可以获得更稳定的能量供给。

再看一下 TypeA 对信号的要求，如图 1.7 所示。

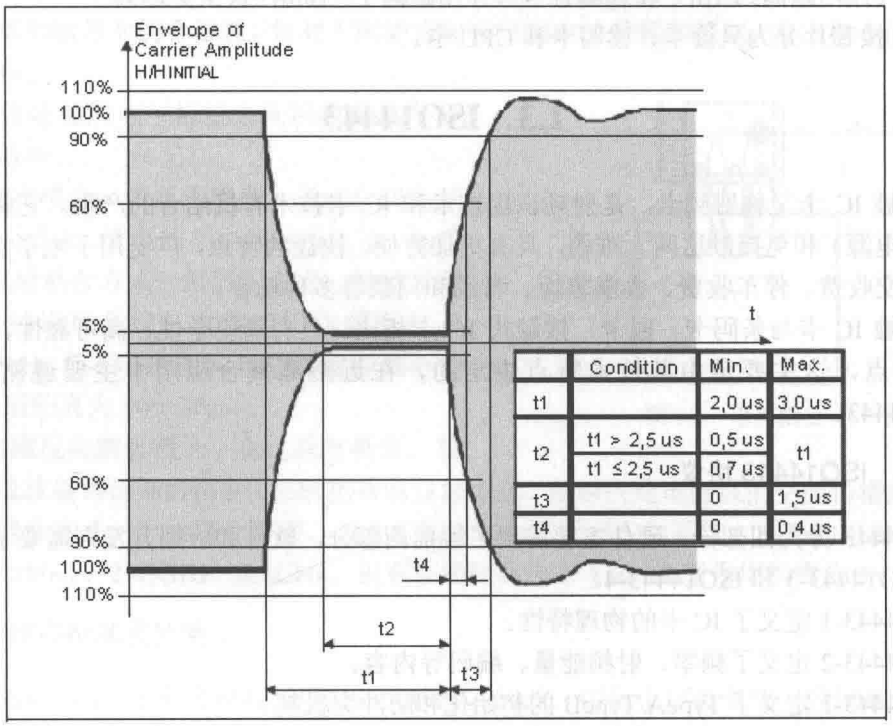

图 1.7　TypeA 信号

它通过一个 2～3μs 的通信间隙来传递数据，这也意味着 PICC 在这个时间间隙中无法得到 PCD 的能量，只能靠卡片内部电容放电来维持内部逻辑电路的工作。

（1）PCD to PICC 即读卡器到射频卡，TypeA 的 PCD 采用改进的米勒（Modified Miller）编码，通信速率为 106Kb/s（13.56MHz/128），码元周期为 9.4μs，调制深度为 100%，ASK 方式。

（2）PICC to PCD 即射频卡到读卡器，TypeA 的 PICC 采用曼彻斯特（Manchester）编码，通信速率也为 106Kb/s，调制深度为 10%，ASK 方式。射频卡到读卡器的信号并非由基带信号直接调制载波信号，而是由 848kHz 的副载波信号对载波信号进行调制。编码定义如下：

PICC to PCD sample (0x0400)

TypeA 使用了半双工通信，通过电磁场传递能量及数据。PCD 和 PICC 通过数据帧交换数据。帧为数据流，TypeA 分为标准帧和短帧。

短帧用于通信初始化，只具有开始位、7 位数据位和结束位，数据部分 LSB 先发送。标准帧用于普通的数据交换，每帧包括开始位、字节数据、校验位和结束位，每个字节数据则包含了 8 位，数据部分 LSB 先发送。

应用中可能有当多张卡同时放置于 PCD 上的情况，这时会产生冲突问题。在 TypeA 中设计了防冲突机制来解决此类问题，且 A 卡使用了比特碰撞检测，速度较快。首先 PCD 发送

REQA（26h），然后放置于 PCD 能量场中的所有 PICC 将同步发出 ATQA（应答），最后，双方进入防冲突循环，PCD 利用 ANTICOLLISION 和 SELECT 命令进行防冲突循环。

根据 TypeA PICC 编码可知，逻辑 1 在码元的前半周期进行调制，而逻辑 0 在码元的后半周期进行调制。如有多张卡片（其 ID 并不相同），则会在某一位产生冲突，具体现象是某一位的前后周期都被调制。PCD 能识别出这个冲突位置，并根据这个值设定 NVB，然后进行 SELECT，如果在 NVB 条件下仍有多张卡片，将会再次产生冲突，此时重复上述循环，直到不再冲突为止，最后选择出最后的卡。

如图 1.8 所示，可看到 Start 位之后出现了连续的调制，而正常数据应该只在前半周期或后半周期进行调制，所以 PCD 此时可判断出比特位冲突。

图 1.8 Type 信号

ISO14443 中的冲突、选卡实例：

PICC 分为 IDLE、READY、ACTIVE、HALT 四个状态。当 PICC 靠近 PCD 并从 PCD 能量场中获得能量后即进入 IDLE 状态，此时卡片可以通过 REQA 和 WUPA 命令进入 READY 状态；READY 状态的卡片接受 PCD 的防冲突选卡，一旦选卡成功，卡片进入 ACTIVE 状态；ACTIVE 状态可进行 ISO14443-4 的操作；在 ACTIVE 状态下，PCD 发出的 HLTA 命令可让卡片进入 HALT 状态，此时需要重新发出 WUPA 命令后才能重新选卡。

有了 HALT 命令，当几个 PICC 放置在 PCD 之上时，可以在用户不移动卡片的条件下，由 PCD 轮流选择卡片使用。

1.3.2 Mifare S50 与 Mifare S70 原理

Mifare S50 和 Mifare S70 又常被称为 Mifare Standard 和 Mifare Classic 或 MF1，是遵守 ISO14443 标准的卡片中应用最广泛、影响力最大的两种。Mifare S70 的容量是 S50 的 4 倍，S50 的容量为 1K 字节，S70 的容量为 4K 字节。阅读器对两种卡片的操作时序和操作命令完全一致。

Mifare S50 和 Mifare S70 的每张卡片上都有一个 4 字节的全球唯一的序列号，卡上数据保存期为 10 年，可改写 10 万次，读无限次。一般的应用中，不用考虑卡片是否会被读坏或写坏的问题，当然，暴力损坏除外。

Mifare S50 和 Mifare S70 的区别主要有两个方面：一是读写器对卡片发出请求命令，二者应答返回的卡类型的字节不同。Mifare S50 的卡类型是 0004H，Mifare S70 的卡类型是 0002H；二是二者的容量和内存结构不同。

Mifare S50 把 1K 字节的容量分为 16 个扇区（Sector0～Sector15），每个扇区包括 4 个数据块（Block0～Block3，我们也将 16 个扇区的 64 个块按绝对地址编号为 0～63），每个数据块包含 16 个字节（Byte0～Byte15），64*16=1024。如表 1.1 所示。

表 1.1 Mifare S50 扇区结构

扇区号	块号		块类型	总块号
扇区 0	块 0	厂商代码	厂商块	0
	块 1		数据块	1
	块 2		数据块	2
	块 3	密码 A　存取控制　密码 B	控制块	3
扇区 1	块 0		数据块	4
	块 1		数据块	5
	块 2		数据块	6
	块 3	密码 A　存取控制　密码 B	控制块	7
…	…	…	…	…
扇区 15	块 0		数据块	60
	块 1		数据块	61
	块 2		数据块	62
	块 3	密码 A　存取控制　密码 B	控制块	63

Mifare S70 把 4K 字节的容量分为 40 个扇区（Sector0～Sector39），其中前 32 个扇区（Sector0～Sector31）的结构和 Mifare S50 完全一样，每个扇区包括 4 个数据块（Block0～Block3），后 8 个扇区每个扇区包括 16 个数据块（Block0～Block15），我们也将 40 个扇区的 256 个块按绝对地址编号为 0～255），每个数据块包含 16 个字节（Byte0～Byte15），256*16=4096。如表 1.2 所示。

表 1.2 Mifare S70 扇区结构

扇区号	块号		块类型	总块号
扇区 0	块 0	厂商代码	厂商块	0
	块 1		数据块	1
	块 2		数据块	2
	块 3	密码 A　存取控制　密码 B	控制块	3
…	…	…	…	…
扇区 31	块 0		数据块	124
	块 1		数据块	125
	块 2		数据块	126
	块 3	密码 A　存取控制　密码 B	控制块	127
扇区 32	块 0		数据块	128
	块 1		数据块	129
	…	…	…	…
	块 14		数据块	142

续表

扇区号	块号		块类型	总块号
	块 15	密码 A 存取控制 密码 B	控制块	143
…	…	…	…	…
扇区 39	块 0		数据块	240
	块 1		数据块	241
	…	…	…	…
	块 14		数据块	254
	块 15	密码 A 存取控制 密码 B	控制块	255

每个扇区都有一组独立的密码及访问控制，放在每个扇区的最后一个 Block 中，这个 Block 又被称为区尾块。S50 的区尾块是每个扇区的 Block3，S70 的前 32 个扇区也是 Block3，后 8 个扇区是 Block15。

S50 和 S70 的 0 扇区 0 块（即绝对地址 0 块）用于存放厂商代码，已经固化，不可更改，卡片序列号就存放在这里。除了厂商块和控制块，卡片中其余的块都是数据块，可用于存储数据。数据块可作两种应用：

（1）用作一般的数据保存，可以进行读、写操作。

（2）用作数据值，可以进行初始化值、加值、减值、读值操作。

数据块和值块有什么区别呢？无论块中的内容是什么，你都可以把它看成普通数据，即使它是一个值块。但并不是任何数据都可以看成是值，因为值块有一个比较严格的格式要求。值块中值的长度为 4 个字节的补码，其表示的范围为-2147483648～2147483647，值块的存储格式如表 1.3 所示。

表 1.3 Mifare 值块存储格式

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
addr	addr	addr	addr	VALUE				VALUE				VALUE			

带下划线表示取反。VALUE 是值的补码，addr 是块号（0～63）。只有具有上述格式，才被认为是值块，否则就是普通的数据块。

每个扇区的区尾块为控制块，包括了 6 字节密钥 A、4 字节存取控制、6 字节密钥 B。例如一张新出厂的卡片控制块内容如图 1.9 所示。

图 1.9 卡片控制内容

新卡的出厂密钥中密钥 A 一般为 A0A1A2A3A4A5，密钥 B 一般为 B0B1B2B3B4B5，或者密钥 A 和密钥 B 都是 6 组 FF。存取控制用以设定扇区中各个块（包括控制块本身）的存取条件，这部分有点复杂，后面将专文介绍。

读写器与 S50 和 S70 的通信流程如图 1.10 所示。

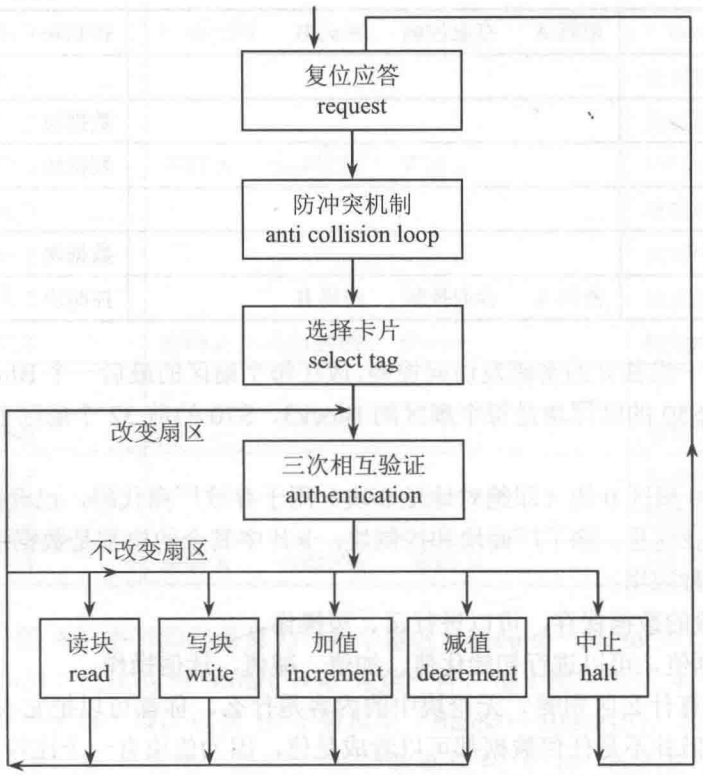

图 1.10　S50 和 S70 的通信流程

卡片选择和三次相互认证在前面已经介绍过。其他操作如下：

（1）读（read）：读取一个块的内容，包括普通数据块和值块。

（2）写（write）：写数据到一个块，包括普通数据块和值块，若值块中写入了非法格式的数据，值块就变成了普通数据块。

（3）加（increment）：对值块进行加值，只能对值块操作。

（4）减（decrement）：对值块进行减值，只能对值块操作。

（5）中止（halt）：将卡置于睡眠工作状态，只有使用 WAKE-UP 命令才能将其唤醒。

事实上加值和减值操作并不是直接在 Mifare 的块中进行的。这两个命令先把 Block 中的值读出来，然后进行加或减，加减后的结果暂时存放在卡上的易失性数据寄存器（RAM）中，然后再利用**传输**（transfer）命令将数据寄存器中的内容写入块中。与**传输**（transfer）相对应的命令是**存储**（restore），作用是将块中的内容存到数据寄存器中，不过这个命令很少用到。

1.3.3　Mifare S50 与 Mifare S70 的存取控制

存取控制是指符合什么条件才能对卡片进行操作。

S50 和 S70 的块分为数据块和控制块，对数据块的操作有“读”“写”“加值”“减值（含传输和存储）”四种，对控制块的操作只有“读”和“写”两种。