摘　要

本文介绍了非接触式 IC 卡技术的基本原理，并对其在工程上的应用作了研究。首先论文描述了 IC 卡的发展和现状。然后通过对射频识别技术原理的研究，揭示了射频 IC 卡的工作原理。本文对 IC 卡中数据的逻辑结构，以及 IC 卡提供的较高的安全性能进行了分析。针对射频 IC 卡所独有的数据传输问题，给出了数据的编码和调制方法，以及防止数据冲突问题的方法。并介绍了射频 IC 卡所必须符合的国际标准 ISO/IEC 14443 的要求，以及 Type A 和 Type B 两种标准的区别。然后预测了非接触式 IC 卡的发展方向——非接触式 CPU 卡技术，并分析了解决射频 CPU 卡能量供给的方法。在最后，以射频 IC 卡在公共汽车自动收费系统中的应用为例，研究了射频 IC 卡的应用问题。其中包括应用系统的整体设计和硬、软件的设计，特别设计了系统的安全性能和系统数据管理的实现方案。并提出了在公共交通领域进行扩展的一卡多用方案。

关键词：非接触式 IC 卡　射频识别　射频 IC 卡　智能卡　一卡多用

Abstract

This paper introduces the basic principle and the application of the contactless IC card technology. First, the paper describes the development and the status quo of the IC cards. Then, the work principle of the radio frequency IC card is discovered through studying the principium of the radio frequency technology. The paper analyzes the logic data structure of the IC card and security performance supported by IC cards. Point to the matters about the data transmission in radio frequency IC cards, the ways to encode and modulate are provides, and the method to anti-collision is presented. The international standards about the radio frequency IC cards – ISO/IEC14443 are introduced too, it refers to the difference about the Type A and Type B standard. Whereafter , the forecast about the trend of the contactless IC cards – contactless CPU cards is given, and the method to solve the power supply problem for radio frequency CPU cards is analyzed. At last, the paper researches the application of radio frequency IC cards with the example of automatic fare collection (AFC) system, the work consists of the hardware and software design, and the whole system structure design. Especially designs the realization of the security performance and the data management. In the end of the chapter, a scheme that fit multi application with single card, which expands the system to the whole public transaction area were brought forward.

Key Word: Contactless IC Card (CICC); Radio Frequency Identification (RFID); Radio Frequency IC Card; Smart Card; Multi Application with Single Card

第一章 绪 论

1.1 什么是IC卡

IC卡是集成电路卡的英文名称，即Integrated Circuit Card的缩写。它是将一个集成电路芯片镶嵌于塑料基片中，封装成卡的形式，其外形与覆盖磁条的磁卡相似，在其左上方嵌有一片或若干片集成电路芯片（接触式IC卡）。芯片一般是不易挥发性存储器（ROM，EPROM，E^2PROM），保护逻辑电路，甚至于CPU（中央处理单元）。

IC卡的概念是20世纪70年代初提出来的，法国布尔（BULL）公司于1976年首先创造出IC卡产品，并将这项技术应用到金融、交通、医疗、身份证明等多个行业，它将微电子技术和计算机技术结合在一起，提高了人们生活和工作的现代化程度[18]。

IC卡芯片具有写入数据和存储数据的能力，IC卡存储器中的内容根据需要可以有条件地供外部读取，或供内部信息处理和判定之用。卡内还存储有唯一的发行人和持卡人的识别标志，用以唯一的确定卡的身份，这样的卡又叫做“识别卡”。

1.2 IC卡的分类

IC卡在经过二十几年的发展之后，逐渐形成了各种类别、不同工作方式的产品系列的家族。因此，对于IC卡的分类也只能从不同的方面进行。

1. 从卡中镶嵌的集成电路的不同分类：IC卡的主要功能就是作为一种数据载体。IC卡内芯片内部电路可分为两大功能：数据存储部分和数据加密操作控制部分。

（1） 存储器IC卡：只有第一部分的则是存储器卡，又称为非加密型存储卡，所用的芯片就是一种串行存储器芯片。

（2） 逻辑加密IC卡：同时具有数据存储部分和数据加密操作控制

部分电路的 IC 卡则是逻辑加密 IC 卡。它是在非加密型存储卡的基础上，在增加一部分加密控制电路。

（3） ASIC 卡（Application Special Integrated Circuit Card）：专用集成电路卡，是在逻辑加密卡的基础上增加上一些专用电路，如完成加密/解密运算的电路等。但由于 ASIC 卡的加解密运算是通过事先设计好的逻辑电路实现的，所以在受到攻击时不能做出相应的变化，对开放式应用环境的安全适应能力不如 CPU 高。

（4） CPU 卡：虽然很多场合下智能卡泛指为大部分的 IC 卡，但是实际上只有 CPU 卡才能真正称得上为智能卡。

CPU 卡在 IC 卡的集成电路中带有微处理器（CPU）电路的 IC 卡。其微处理器单元一般为 8 位微处理器，能执行指令和程序。

CPU 卡属于主动型。它不仅能够管理各种输入/输出的数据，检验来自接口设备的输入的个人密码，而且能够根据应用系统的要求主动识别与之连接的接口设备。因此，在 CPU 卡中，能够建立多种应用系统的授权，存放多个应用系统的相关数据，并实现对数据信息存取的高可靠性、高安全性控制，可以进行复杂的信息处理和计算。这种 IC 卡可以以一种新型的金融交易卡——现金卡（Cash Card）的方式，完全代替现金进行消费和支付，成为真正的“电子货币”。

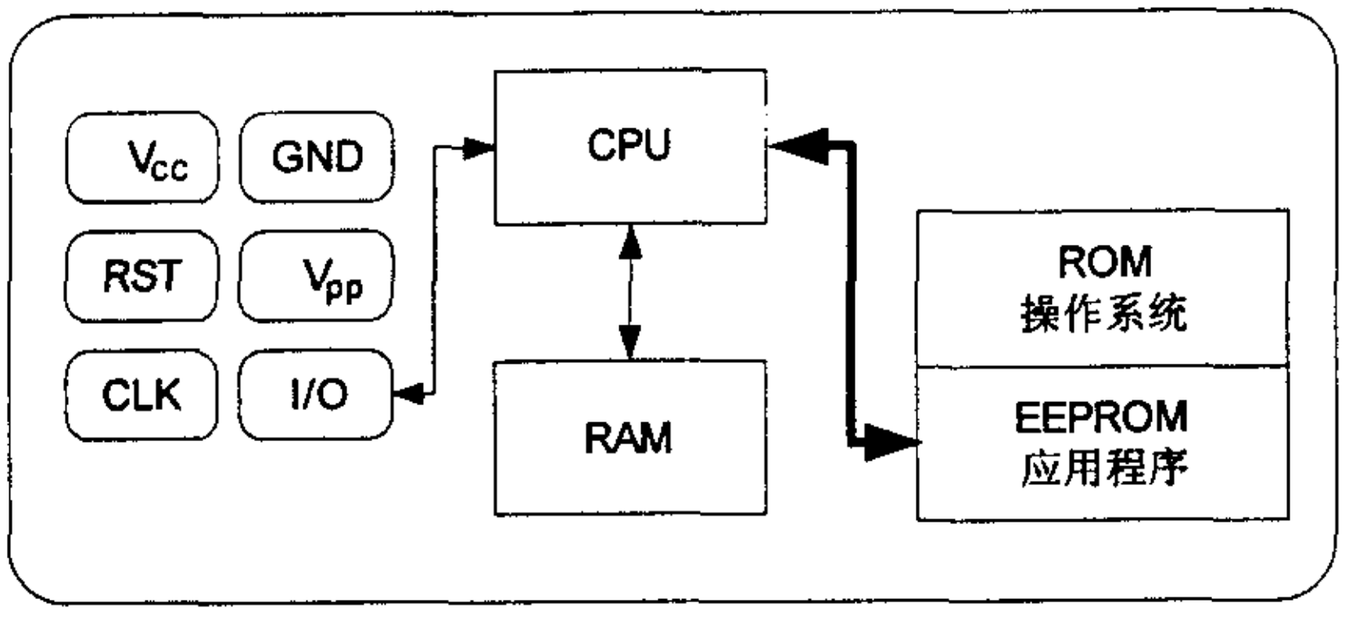


图1.1 CPU卡的典型结构

2. 按应用领域来分：

IC 卡有金融卡和非金融卡两种。金融卡又有信用卡（credit card）和现金卡（debit card）等。非金融卡往往出现在各种事物管理、安全管理场所，如身份证明、健康记录和职工考勤等。另外一些预付费卡，如用于公交系统中的交通卡和电表上的 IC 卡等，各有相应的管理单位发行（当然

也可委托银行收费），这种卡兼有一部分电子钱包的功能。

3. 从硬件角度进行划分：图 1.2 为从硬件角度对 IC 卡分类的分类表。

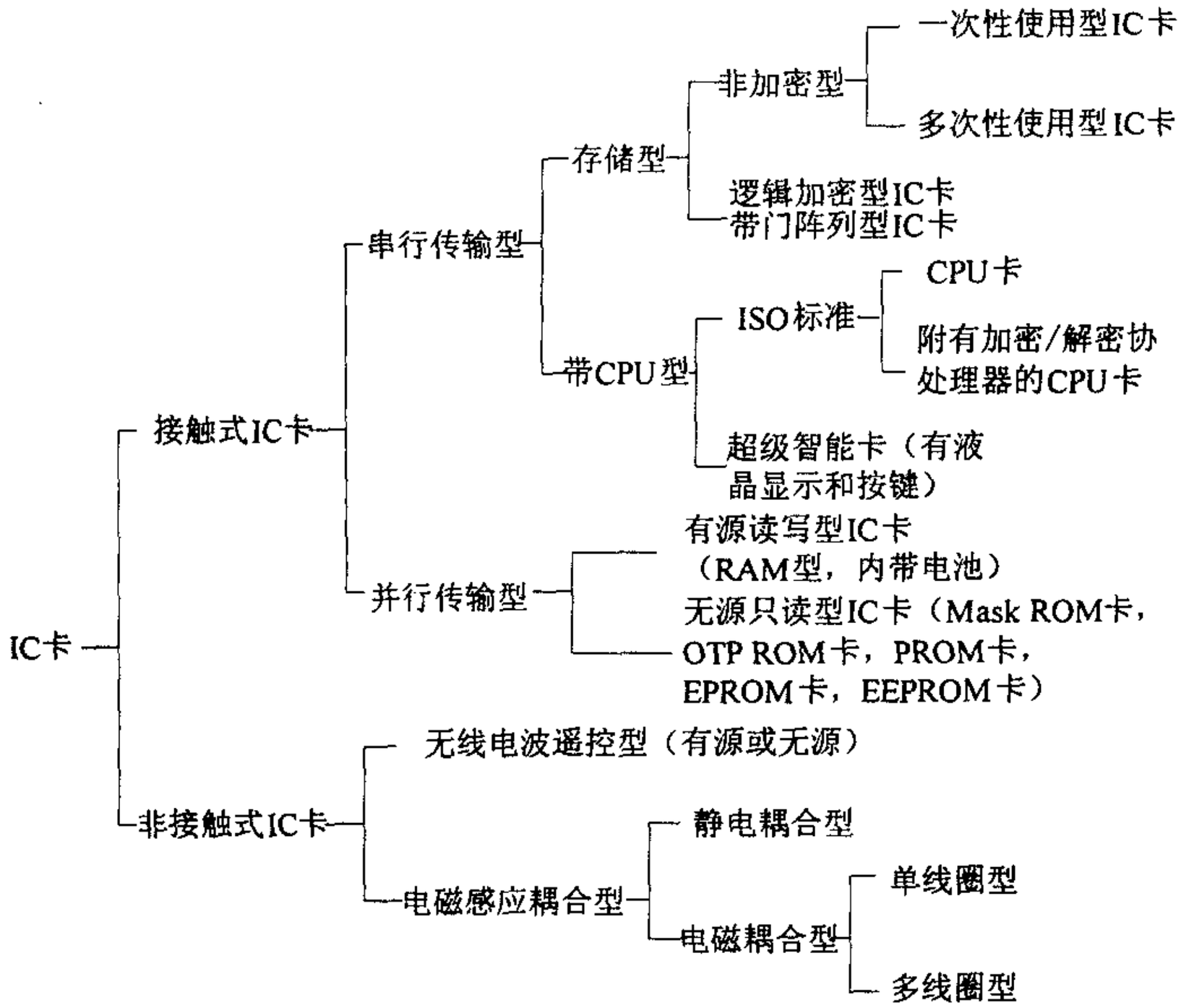


图1.2 从硬件角度对IC卡进行分类

1.3 非接触式 IC 卡

从图 1.2 中可以看到，IC 卡可以从硬件角度分为接触式和非接触式两大类。其中通过卡芯片上的 6 个或 8 个触点来实现与读卡器进行数据传送的为接触式 IC 卡。而非接触式的 IC 卡（contactless IC cards）在集成电路上不向外引出触点，而是通过包含在卡片中的无线收发电路及相关的一些电路来实现与外界的数据交流和电源的供给，其通过无线电波或电磁场感应的方式进行能量和数据的交换。本文将主要对非接触式 IC 卡及其应用进行研究，特别是其中的电磁耦合型，也就是当今用得比较多的射频 IC 卡（Radio Frequency IC cards）。在下一章当中将对射频 IC 卡的基础—射频识别技术做一些介绍。

第二章　射频识别技术

2.1　什么是射频识别

对于接触式 IC 卡来说，在很多情况下，机械触点的接通是不可靠的。数据载体与一个所属的阅读器之间的数据进行非接触传输将灵活得多。电子数据载体工作时所需要的能量通过阅读器非接触地传输来获取。根据使用的能量和数据传输方法，我们把非接触的识别系统称作射频识别系统（RFID—Radio Frequency Identification）。

2.1.1 射频识别系统（RFID）及其组成

射频识别系统与 IC 卡有着密切的关系。数据存储在电子数据载体（称应答器）之中。然而，应答器的能量供应以及应答器与阅读器之间的数据交换不是通过电流的触点接通而是通过磁场或电磁场，这方面采用了无线电和雷达技术。射频识别是无线电频率识别的简称，即通过无线电波进行识别。同其他识别系统相比，射频识别系统具有许多优点。因此，射频识别系统开始占领了巨大的销售市场。这方面的典型例子是：用非接触式 IC 卡作短距离公交车票[23]。

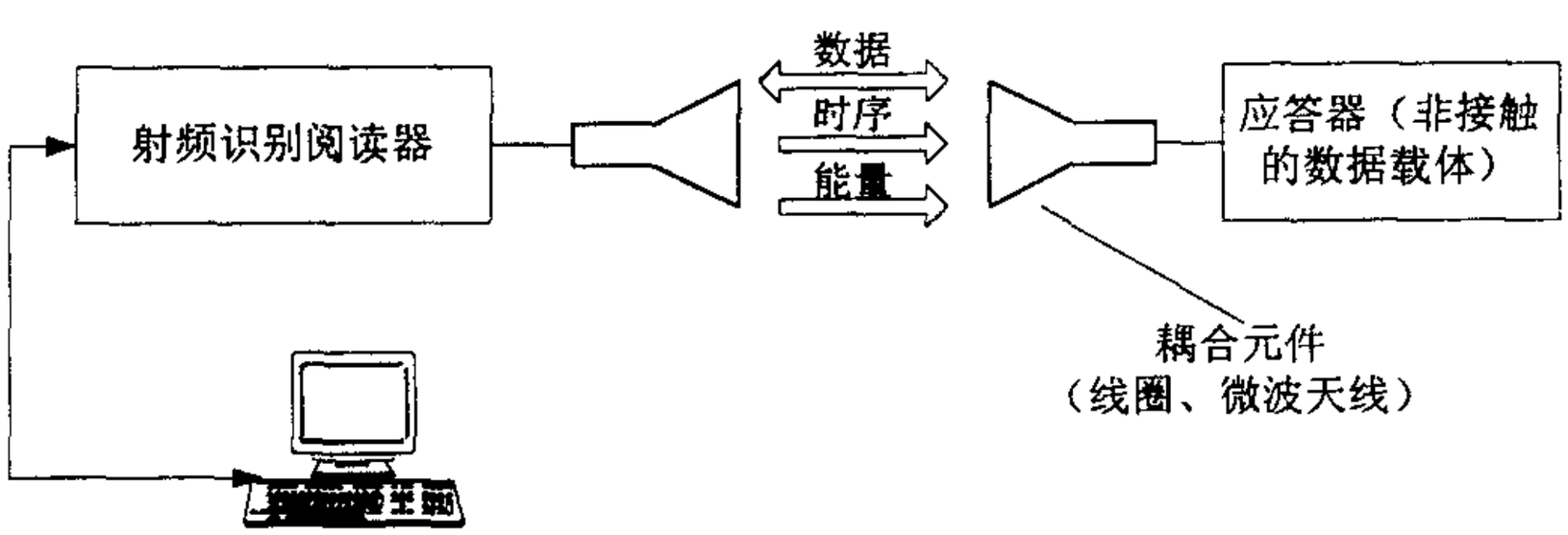


图2.1 阅读器和应答器是各种射频识别系统的基本组成部分

射频识别系统（图 2.1 所示）一般由以下两部分构成：

应答器：应答器应放置在要识别的物体上；

阅读器：阅读器可以是读或写/读装置，取决于所使用的结构和技术。一台典型的阅读器包含有高频模块（发射器和接收器）、控制单元以

及与应答器连接的耦合元件。此外，许多阅读器还带有附加的接口（RS 232, RS 485 等），以便将所获得的数据进一步传输给另外的系统（个人计算机、机器人控制装置等）。

应答器是射频识别系统真正的数据载体。通常，应答器由耦合元件以及微电子芯片组成。在阅读器的响应范围之外，应答器处于无源状态。一般，应答器没有自己的供电电源（电池）。只有在阅读器的响应范围之内，应答器才是有源的。应答器工作所需的能量，如同时钟脉冲和数据一样，是通过耦合单元（非接触的）传输给应答器的。

2.1.2 各种射频识别系统的区别

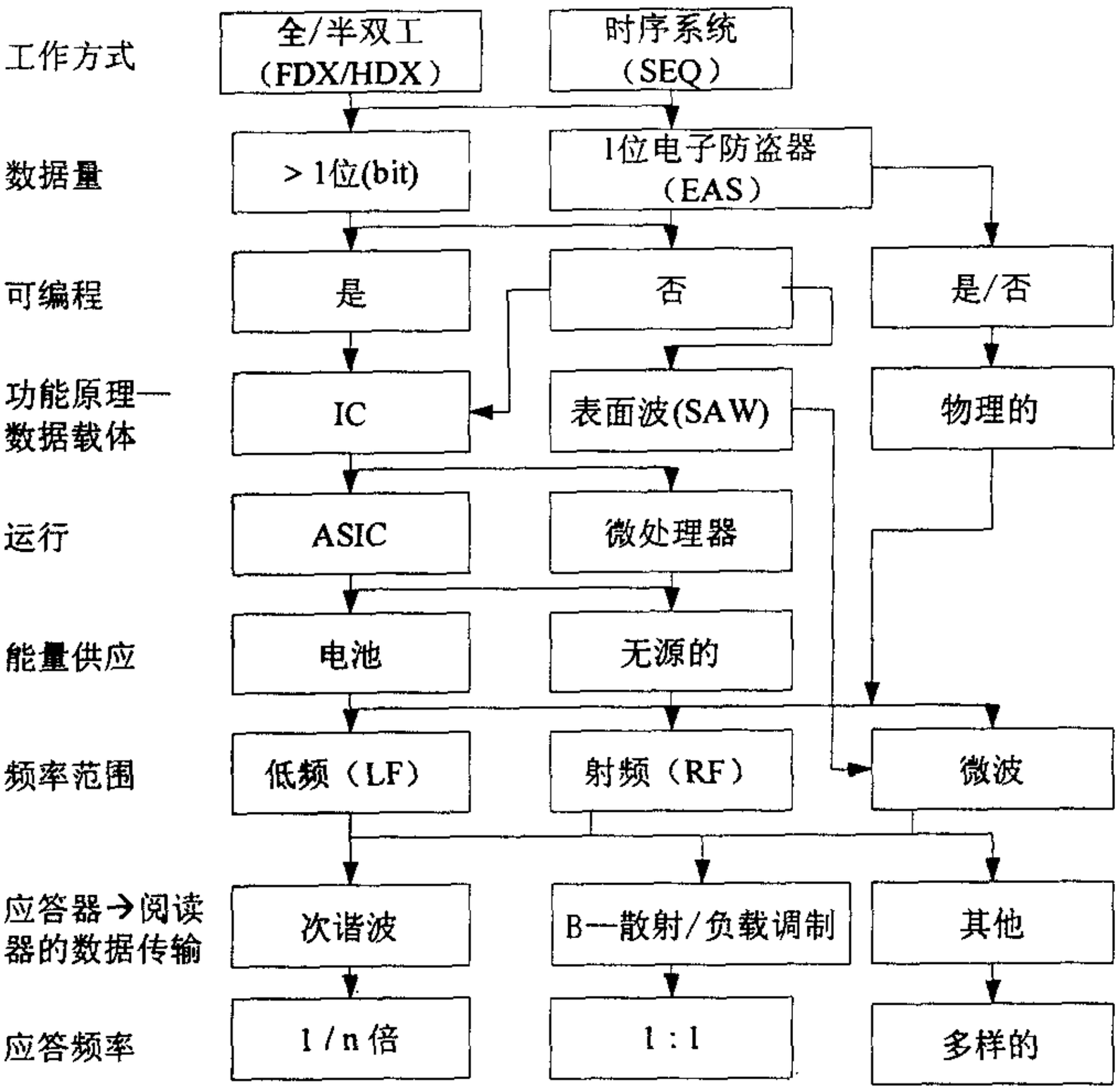


图2.2 射频识别系统的各种区别特征[37]

射频识别系统包含了许多不同改型的品种，有众多厂家生产。为了了

及与应答器连接的耦合元件。此外，许多阅读器还带有附加的接口（RS 232, RS 485 等），以便将所获得的数据进一步传输给另外的系统（个人计算机、机器人控制装置等）。

应答器是射频识别系统真正的数据载体。通常，应答器由耦合元件以及微电子芯片组成。在阅读器的响应范围之外，应答器处于无源状态。一般，应答器没有自己的供电电源（电池）。只有在阅读器的响应范围之内，应答器才是有源的。应答器工作所需的能量，如同时钟脉冲和数据一样，是通过耦合单元（非接触的）传输给应答器的。

2.1.2 各种射频识别系统的区别

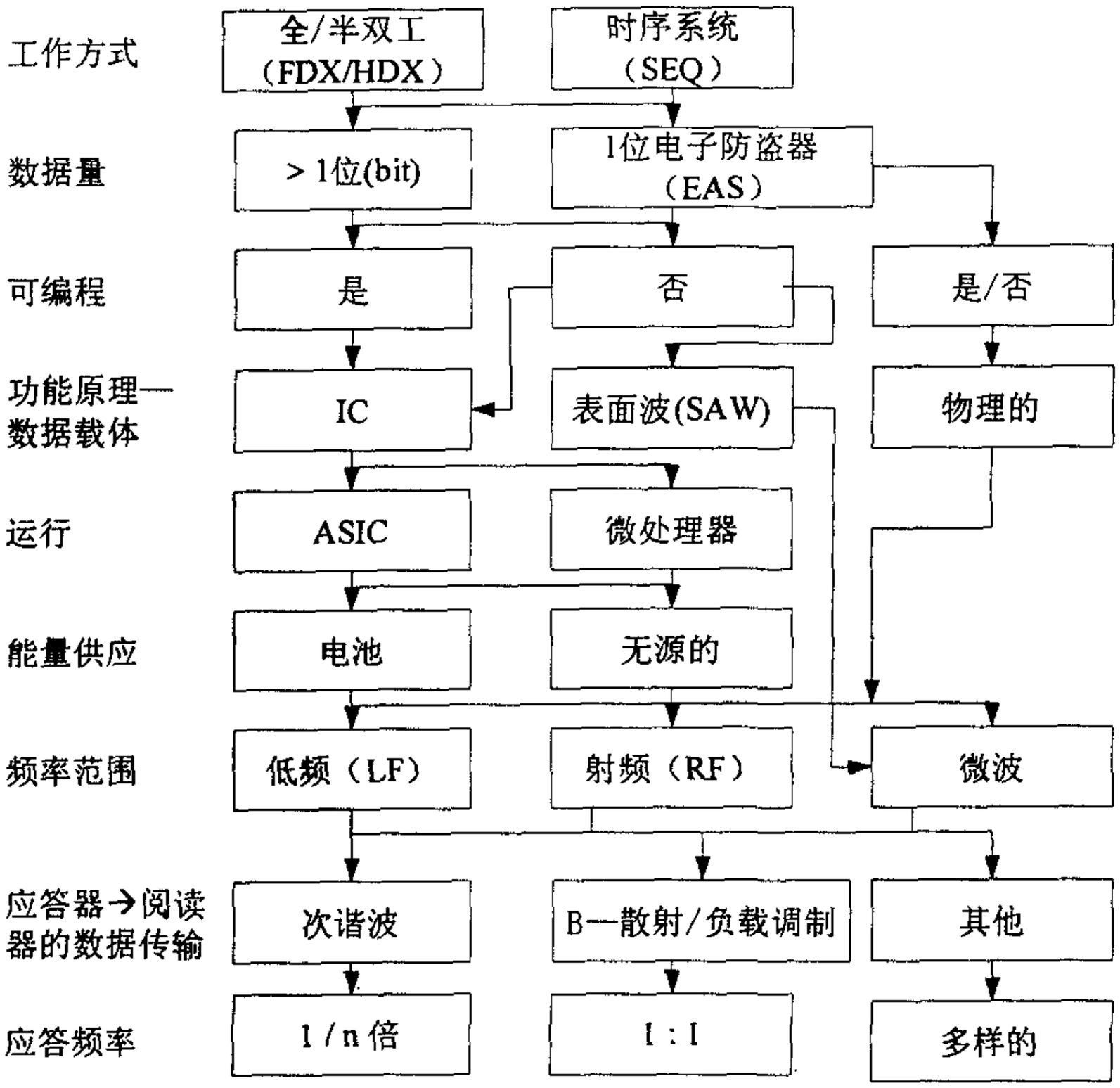


图2.2 射频识别系统的各种区别特征[37]

射频识别系统包含了许多不同改型的品种，有众多厂家生产。为了了

解射频识别系统的全貌，需要找出能把各种射频识别系统相互区别开来的特征[2]。在图 2.2 中最左边一列给出了射频识别系统的分类特征，而右边的方框中描述了这些分类特征所具有的不同种类，顺着箭头从上至下可以将各个具体的分类特征综合起来，而形成射频识别系统中的一个体系。

就射频识别系统的基本工作方式来说，分为全双工（FDX）和半双工（HDX）系统以及时序（SEQ）系统。

在全双工和半双工系统中，应答器的应答响应是在阅读器接通高频电/磁场的情况下发送出去的。因为与阅读器本身的信号相比，应答器的信号在接收天线上是很弱的，所以必须使用合适的传输方法，以便把应答器的信号与阅读器的信号区别开来。在实践中，人们对从应答器到阅读器的数据传输使用负载调制，有副载波的负载调制，还有阅读器发射频率的谐波。

时序方法则与之相反，阅读器的电/磁场短时间周期地断开。这些间隔被应答器识别出来，并被用于从应答器到阅读器的数据传输。时序方法的缺点是：在阅读器发送间歇时，应答器的能量供应中断，这就必须装入足够大的辅助电容器或辅助电池进行补偿。

射频识别应答器的数据量通常是几个字节到几千个字节之间。但是，有一个例外，这就是 1 比特应答器。它有 1 比特的数据量就足够了，使阅读器能发出两种状态的信号："在电磁场中有应答器"或"在电磁场中无应答器"。这对于实现简单的监控或信号发送功能是完全足够的。

能否给应答器写入数据是区分射频识别系统的另外一个因素。对很简单的系统来说，应答器的数据组大多是很简单的（序列）号码，是在加工芯片时集成进去的，以后不能改变。与此相反，可写入的应答器通过阅读器写入数据。对电感耦合的射频识别系统来说，使用电可擦可编程存储器（EEPROM）是主要的方法。然而，使用这种方法的缺点是：写入过程中的功率消耗很大，使用寿命最高为写入 100，000 次。另外一种铁电随机存取存储器（FRAM），与电可擦可编程只读存储器相比写入功率消耗减少 100 倍，写入时间甚至减少 1000 倍[32]。

对可编程系统来说，必须由数据载体的"内部逻辑"控制对存储器的写读操作以及对写/读授权的请求。在最简单的情况下，可以由 ASIC（专用集成电路）来完成，使用 ASIC，可以完成很复杂的过程。然而，ASIC 的缺点是：对修改编程的功能缺乏灵活性，这意味着要设计制造新的芯片，

由于这些变化需要修改硅芯片上的电路，因而要花费大量钱财。

微处理器的使用明显地改善了这种情况。在芯片生产时，将用于管理应用数据的操作系统，通过掩膜的方式集成到微处理器中，这种修改花费不多。此外，软件还能调整以适合各种专门应用。

人们把用 ASIC 控制的可写入数据载体也称作“存储器卡”，以便和“CPU 卡”区分开来。

射频识别系统的另一重要特征是系统的工作频率和作用距离。通常把阅读器发送时使用的频率称作射频识别系统的工作频率。不考虑应答器的发送频率，在大多数情况下，把它叫做阅读器发送频率（负载调制、反向散射）。然而，在任何情况下，应答器的“发射功率”会比阅读器的发射功率低几十个百分点。

各种发送频率基本上划归三个范围：低频（30kHz~300kHz）、高频或射频（3MHz~30MHz）和超高频（300MHz~3GHz）或微波（>3GHz）。根据作用距离，射频识别系统的附加分类是：密耦合（0~1cm）、遥耦合（0~1m）和远耦合（>1m）。

按应答器回送到阅读器的数据传输的各种方法可以分为三类：应用反射或反向散射（反射波的频率与阅读器的发送频率一致即频率比为 1:1）或负载调制（阅读器的电/磁场受应答器的影响→频率比为 1:1），分谐波（1/n 倍）以及应答器中产生的高次谐波（n 倍）。

2.2　射频系统的频率、作用距离和耦合

1．密耦合

具有很小作用距离的射频识别系统，典型的范围从 0 到 1cm，人们把这种系统称作密耦合系统。必须把应答器插入阅读器中，或者放置在阅读器为此设定的表面上。

密耦合系统可以用介于直流和 30MHz 交流之间的任意频率进行工作，因为应答器工作时不必发射电磁波。数据载体与阅读器之间的紧密耦合能够提供较大的能量，甚至可供电流消耗较大的微处理器进行工作。密耦合系统应用于安全要求较高，但不要求作用距离的设备中。例如：电子门锁系统或带有计数功能的非接触式 IC 卡系统。目前，密耦合应答器只作为 ID-1 格式的非接触式 IC 卡使用。

2．遥耦合

把写和读的作用距离增至 1m 的系统称作遥耦合系统。所有遥耦合系统在阅读器和应答器之间都是电感（磁）耦合。因此，人们也把这些系统称作电感无线电装置。所有出售的射频识别系统的 90%~95%都属于电感（磁）耦合系统（见图 2.3）。

作为发送频率，使用 135kHz 以下的频率，或使用 6.75MHz、13.56 MHz 以及 27.125 MHz 频率。按应答器到阅读器的距离来说，通过电感耦合可传输的能量是很小的，以致往往只使用耗电很少的只读数据载体。使用微处理器应答器的高档系统也属于电感耦合系统范围之内。

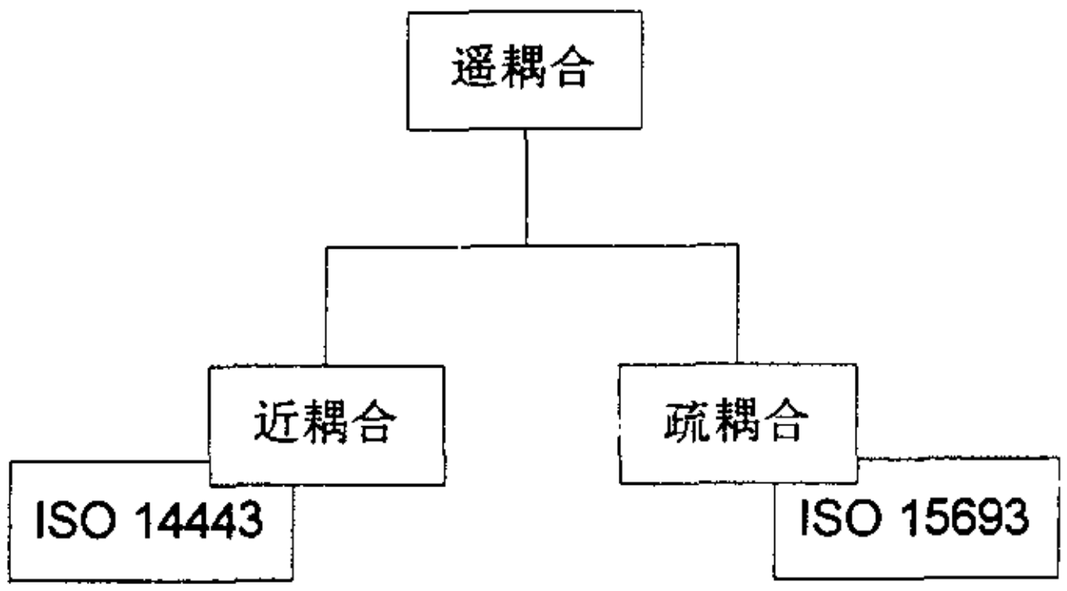


图2.3 对非接触式IC卡来说，近耦合（典型距离为15cm）与疏耦合（大约距离为1m）是有区别的

3．远距离系统

远距离系统典型的作用距离是从 1m 到 10m，个别的系统也有更远的作用距离。所有远距离系统都是在微波范围内用电磁波工作的，发送频率通常为 2.45GHz，众所周知，也有些系统使用的频率为 915MHz，5.8 GHz 和 24.125 GHz。

为了应答器和阅读器之间的联系，只能使用高频能量，该能量由阅读器接收。因此，把反向散射方法作为由应答器到阅读器的数据传输的标准方法。

2.3 射频识别系统的基本作用原理

2.3.1 全双工和半双工

对于非接触式 IC 卡来说，它的应答器是用一个微型芯片来做数据载

体的，在这个数据载体上，存储的数据量可达数千字节。为了读出或写入数据，必须在应答器和阅读器之间能够传输数据。数据传输使用了两种基本不同的方法：全双工和半双工。

在半双工法（HDX）中，从应答器到阅读器的数据传输与从阅读器到应答器的数据传输是交替进行的。当频率在 30MHz 以下时常常使用负载调制的半双工法，有没有副载波都无所谓，电路也很简单。负载调制和调制反射截面直接影响由阅读器产生的磁场或电磁场，因此被称作“谐波”处理法。

在全双工法（FDX）中，数据在应答器和阅读器之间的双向传输是同时进行的。其中包括应答器发送数据，所用频率为阅读器的几分之一，即采用“分谐波”，或是用一种完全独立的“非谐波”频率。

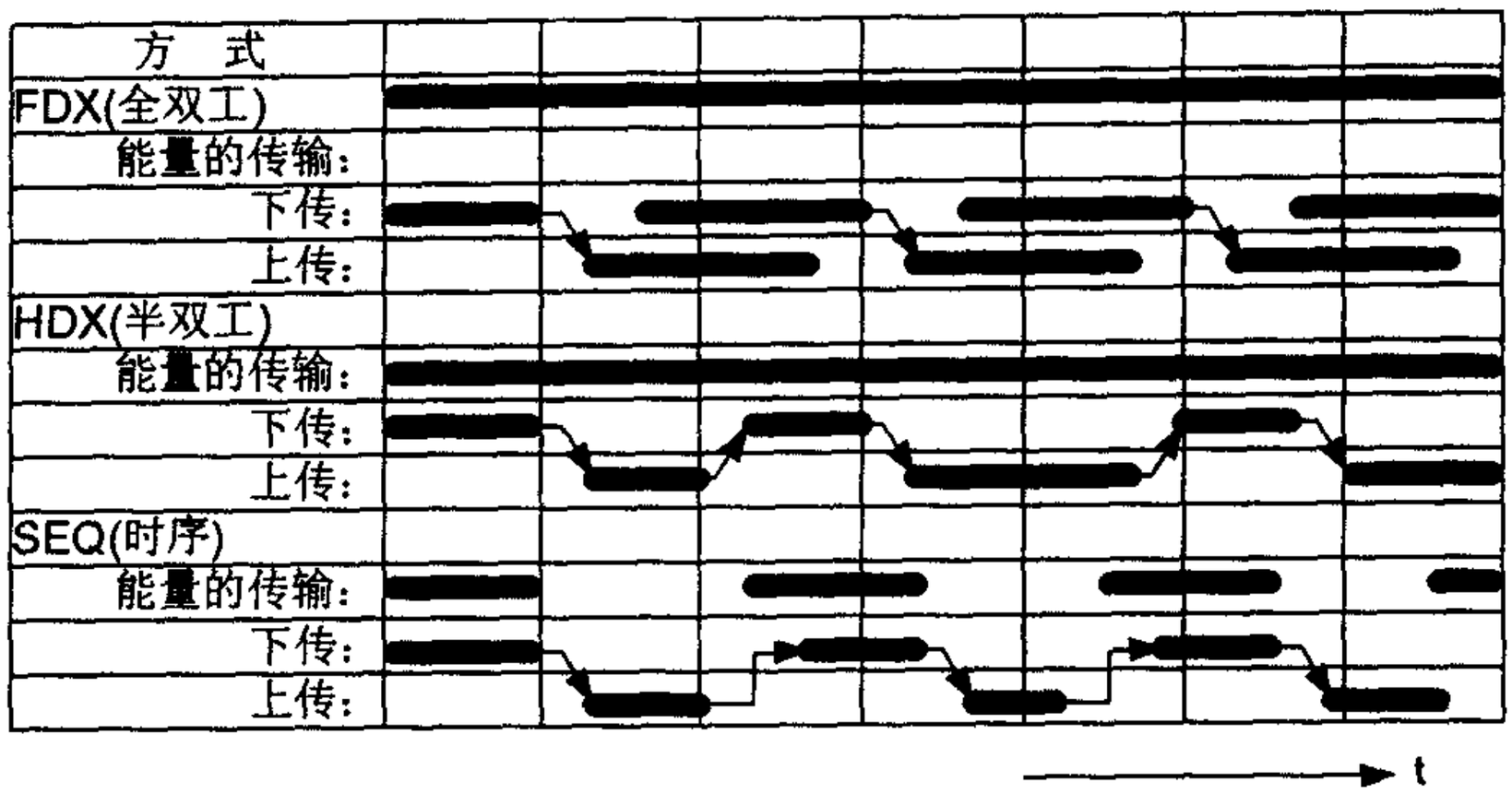


图2.4 全双工系统、半双工系统和时序系统的时间过程说明

这两种方式的共同点是：从阅读器到应答器的能量传输是连续的，与数据传输的方向无关。与此相反，在使用时序系统的情况下，从阅读器到应答器的能量传输总是在限定的时间间隔内进行的（脉冲操作→脉冲系统）。从应答器到阅读器的数据传输是在应答器的能量供应间歇时进行的。如图 2.4 所示：

在图中，人们把从阅读器到应答器的数据传输称作下传，把从应答器到阅读器的数据传输称作上传。

1．电感耦合

1）无源应答器的能量供应

电感耦合应答器由一个电子数据载体，通常是由单个微型芯片以及用作天线用的大面积的线圈等组成。

电感耦合应答器几乎都是无源工作的。这意味着：微型芯片工作所需要的全部能量必须由阅读器提供。高频的强电磁场由阅读器的天线线圈产生，这种磁场穿过线圈横截面和线圈周围的空间。因为使用频率范围（<135kHz：2400m，13.56MHz：22.1m）内的波长比阅读器天线和应答器之间的距离大好多倍，可以把应答器到天线的距离间的电磁场当作简单的交变磁场来对待。

发射磁场的一小部分磁力线穿过距阅读器天线线圈一定距离的应答器天线线圈。通过感应，应答器的天线线圈上产生一个电压 U_i。将其整流后作为数据载体（微型芯片）的电源。将一个电容器 C_r 与阅读器的天线线圈并联，电容器电容的选择依据是：它与天线线圈的电感一起，形成谐振频率与阅读器发射频率相符的并联振荡回路。该回路的谐振使得阅读器天线线圈产生非常大的电流，这种方法也可用于产生供远距离应答器工作所需要的场强。

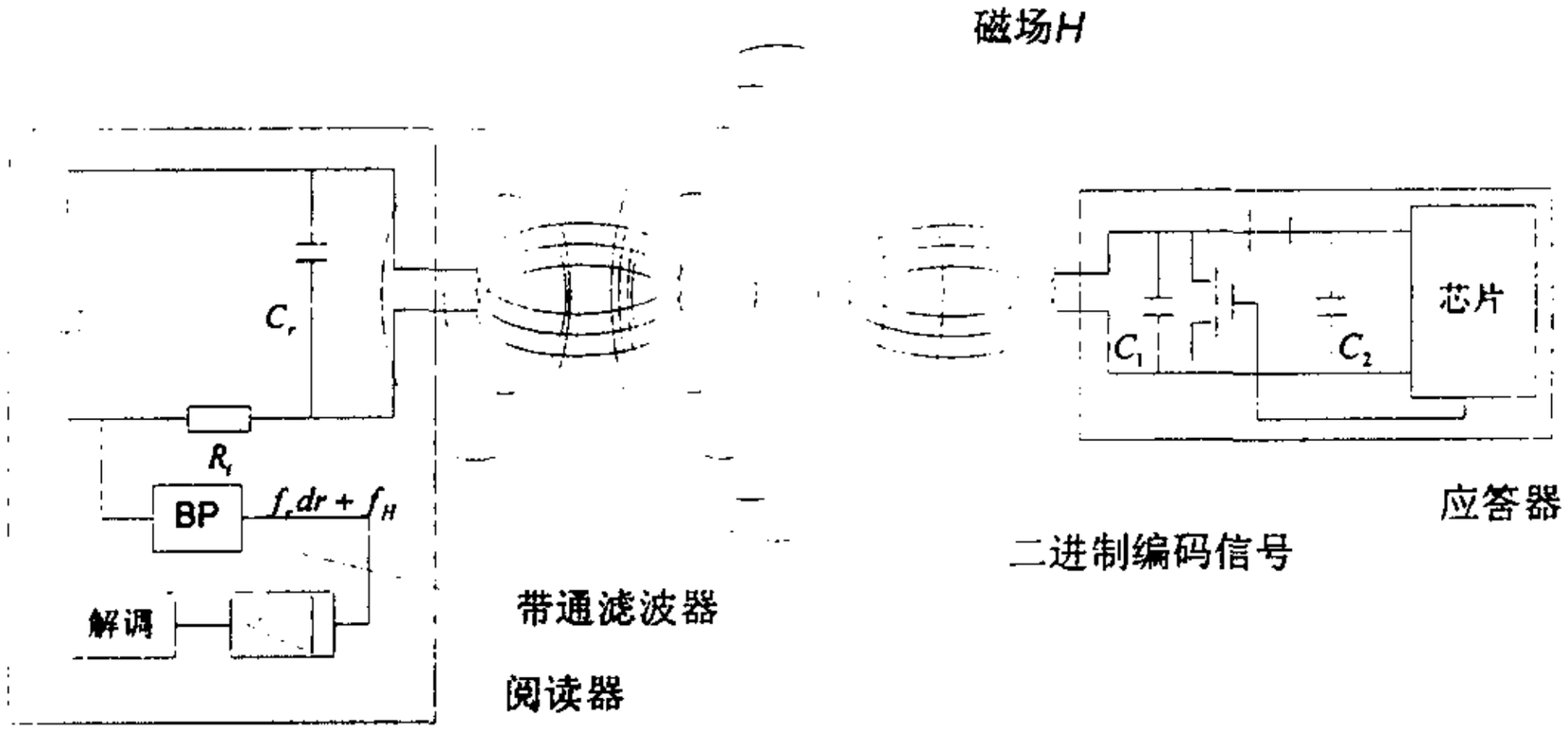


图2.5 通过芯片上场效应管源—漏电组的变换在应答器中产生负载调制（图中阅读器是为检测副载波设计的）

应答器的天线线圈和电容器 C_1 构成振荡回路，调谐到阅读器的发射频率。通过该回路的谐振，应答器线圈上的电压 U 达到最大值。

这两个线圈的结构也可以解释作变压器（变压器的耦合），变压器的两个线圈之间只存在很弱的耦合。阅读器的天线线圈与应答器之间的功率

传输效率与工作频率 f、应答器线圈的匝数 n、被应答器线圈包围的面积 A、两个线圈的相对角度以及它们之间的距离成比例[7]。

随着频率的增加，所需的应答器线圈的电感，表现为线圈匝数“N”的减少（135kHz 典型为 100~10000 匝，13.56MHz：典型为 3~10 匝）。因为应答器中的感应电压是与频率成比例的，在较高频率的情况下，线圈匝数较少对功率传输效率几乎没有影响。

因为电感耦合系统的效率不高，所以只适用于低电流电路。只有功耗极低的只读应答器（<135kHz）可用于 1m 以上的距离。具有写入功能和复杂安全算法的应答器的功率消耗较大，因而一般的作用距离为 15cm，尽管个别的可达到 80cm[3]。

2）应答器至阅读器的数据传输

（1）负载调制：对电感耦合系统来说是一种变压器耦合型，即作为初级线圈的阅读器和作为次级线圈的应答器之间的耦合。只要线圈之间的距离不大于 0.16λ（波长），并且应答器处于发送天线的近场之内，变压器耦合就是有效的。

如果把谐振的应答器（就是说，应答器的固有谐振频率与阅读器的发送频率相符合）放入阅读器天线的交变磁场中，那么该应答器就从磁场取得能量。从供应阅读器天线的电流在阅读器内阻 R_i 上的压降可以测得此附加功耗。应答器天线上的负载电阻的接通和断开促使阅读器天线上的电压发生变化，实现用远距离应答器对天线电压进行振幅调制。如果人们通过数据控制负载电压的接通和断开，那么这些数据就能够从应答器传输到阅读器。人们把这种数据传输方式称作负载调制。

为了在阅读器中回收数据，需要对在阅读器天线上测得的电压进行整流。这意味着对经过振幅调制的信号进行解调。

（2）使用副载波的负载调制：由于阅读器天线与应答器天线之间的耦合很弱，阅读器天线上表示有用信号的电压波动在数量级上比阅读器的输出电压小。实践中，对 13.56MHz 的系统来说，当天线电压大约为 100V（通过谐振使电压升高）时，只能得到大约为 10mV 的有用信号（等于 80dB 有用信号/“干扰信号”之比）。因为检测这些很小的电压变化需要在电路上花费巨大开销，所以人们利用由天线电压振幅调制所产生的调制波边带。

如果应答器的附加负载电阻以很高的时钟频率 f_H 接通或断开，那么

在阅读器发送频率±f_H的距离上产生两条谱线，他们是容易检测到的（然而，必须是$f_H < f_{阅读器}$）。在无线电技术的术语中，把这种新的基本频率称作副载波。数据传输是及时在数据流中通过振幅键控（ASK）、频移键控（FSK）和相移键控（PSK）调制来完成的，这就是副载波的振幅调制。

通过使用副载波的负载调制，在阅读器天线上和在工作频率两侧副载波频率$f_{阅读器}$的距离上，产生两条调制波边带。通过在两个频率$f_{阅读器} \pm f_H$之一的带通滤波器（BP），这两条调制波边带可以与阅读器的较强的信号分开，在放大后，可以很容易地解调副载波信号。

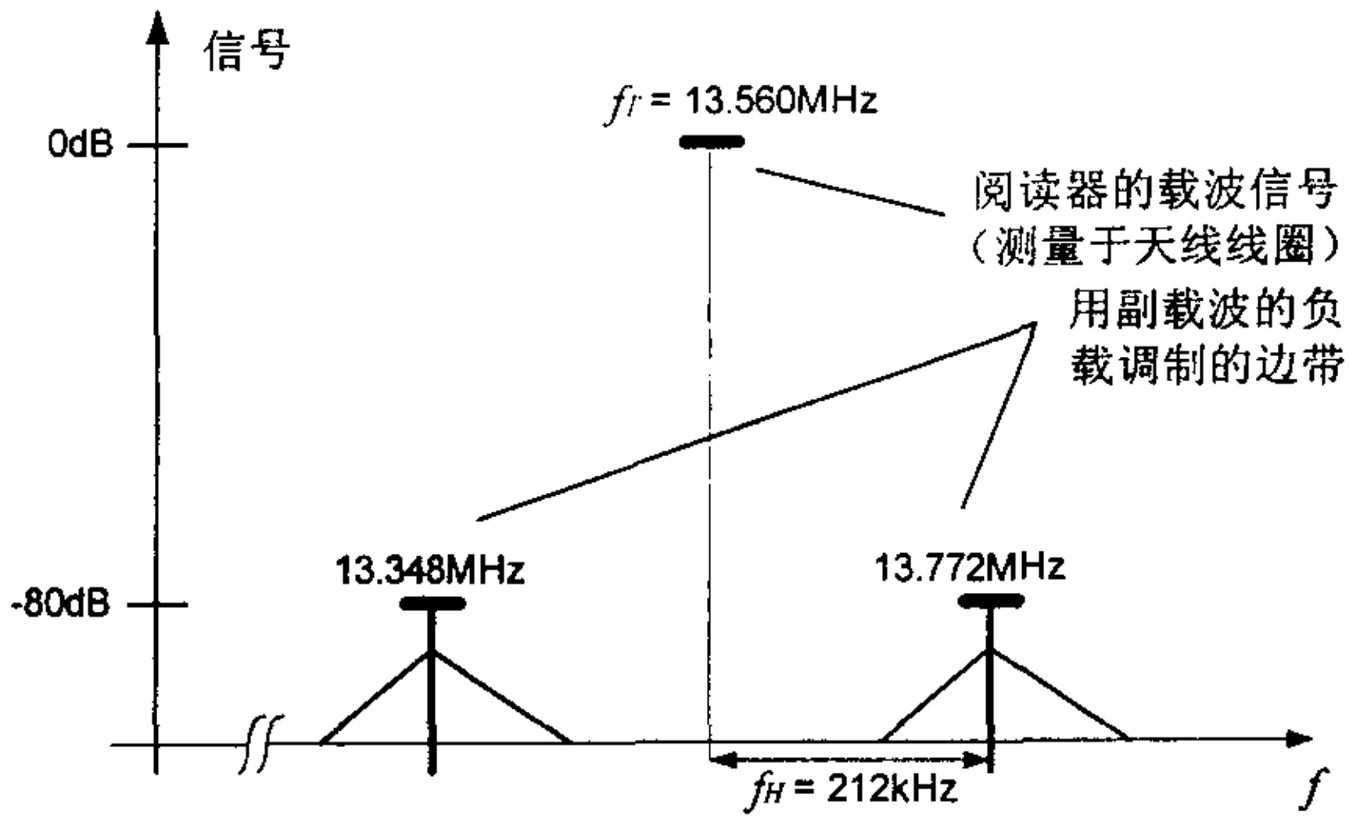


图2.6 通过使用副载波的负载调制，在阅读器的发送频率两侧相距副载波频率f_S处产生两条波边带（真实的信息在两条副载波的边带中，副载波的边带是通过自身的调制而产生的）

2. 电磁反向散射耦合

1）应答器的能量供应

阅读器与应答器之间的作用距离在1m以上的射频识别系统被称作远距离系统。这些系统用433MHz和5.6GHz之间的频率进行工作。

这些频率范围的短波波长使人们设计尺寸较小、效率较高的天线，使用的频率范围可以是小于135kHz和13.56MHz。通过远距离场随距离的衰减的计算，可以估计从阅读器到应答器的功率传输效率。当工作频率为2.45GHz而发送天线和接收天线之间的距离为10m时，线路衰减大约为60dB。如果我们假设微型芯片的功耗大约为10μW（可以用一个功能相同的电感耦合的应答器的功率消耗作比较），那么在阅读器上发射的功率必须是10W（等于10μW+60dB）等效发射功率（ERP）。

2）应答器至阅读器的数据传输

调制的反射横截面—从雷达技术中得知：电磁波被大小超过波长一半的物体所反射。一个物体反射电磁波的效率是通过其反射横截面来说明的。物体同到达它的波前产生谐振时，其反射横截面尤其大，这正是处于适当的频率的天线所用的场合。

功率 P_1 是从阅读器天线发射出来的，它的一小部分（自由空间衰减）到达应答器的天线。到达应答器的功率 P_1' 作为 HF 电压在天线接口处供使用，经二极管 D_1 和 D_2 整流后，可作为操作电压以去活化/活化省电的“低功耗”模式。这里使用的二极管是低阻挡层肖特基二极管，这种二极管具有极低的门槛电压。所获得的电压足够用作短作用距离的能量供应。到达的功率 P_1' 一部分被天线反射，返回功率为 P_2。天线的反射性能（等于反射横截面）会受到连接到天线的负载变化的影响。为了从应答器到阅读器传输数据，与天线并联的附加负载电阻 R_L 的接通和断开要和传输的数据流一致，从而完成对由应答器反射的功率 P_2 振幅的调制（调制后的反向散射）。

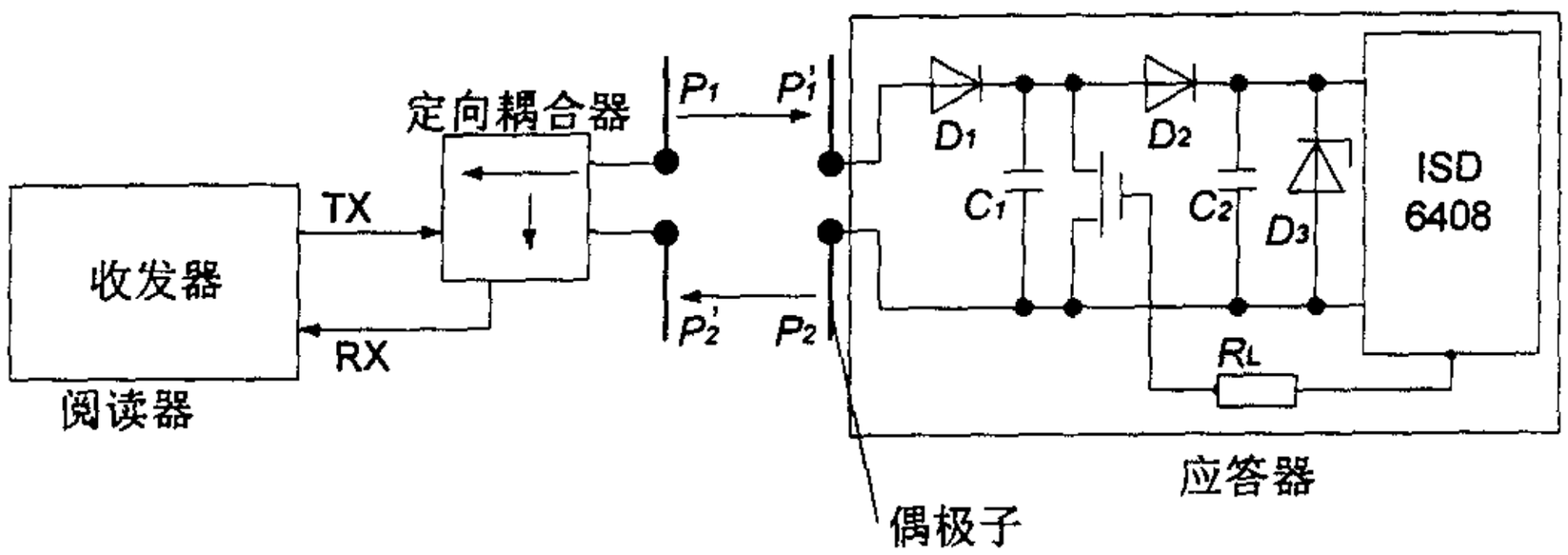


图2.7 反向散射应答器的作用原理（通过芯片上的场效应晶体管的换接“调制”芯片的阻抗）[37]

由应答器反射的功率 P_2 在空间自由辐射。其中的一小部分（自由空间衰减）被阅读器天线接收。反射信号以“相反的方向”进入阅读器的天线连接处，被定向耦合器解耦后，送到阅读器的接收入口。发射器的强大了十次幂的“前进”信号通过定向耦合器在很大程度上受到了抑制。

由阅读器发射的功率和由应答器返回的功率之比（P_1/P_2'）可以根据雷达方程进行估算。

3．密耦合

1）应答器的能量供应

密耦合系统是为从 0.1cm 到最大 1cm 的作用距离设计的。因此，工作时需要将应答器插入阅读器之中，或放到一个有标记的表面上。应答器插入阅读器之中或放到使应答器线圈能在环形铁芯或 U 性铁芯的能准确定位的缝隙中。应答器线圈和阅读器线圈的功能结构相应于变压器。阅读器线圈相当于变压器的初级线圈，应答器线圈相当于变压器的次级线圈。通过初级线圈的高频电流，在这样安排的铁芯和气隙中产生高频磁场。这种高频磁场也穿过应答器线圈，并在应答器线圈中感应出频率相同的交流电压。对此电压整流，可获得供芯片使用的电源电压。

由于在应答器线圈中感应的电压 U 与激励电流的频率 f 成正比，所以应当为能量传输选择尽可能高的频率。在实践中，使用从 1~10MHz 范围的频率。为了使变压器铁芯中的损耗很小，必须使用合适的铁氧体作铁芯材料。

4．阅读器到应答器的数据传输

在全双工系统和半双工系统中，所有已知的数字调制方法都可用于从阅读器到应答器的数据传输，而与工作频率或耦合方式无关。大致可以区分为以下三种基本方法：

- ASK：振幅键控
- FSK：频移键控
- PSK：相移键控

为了便于解调，多数系统使用振幅键控调制。

2.3.2 时序法

如果从阅读器到数据载体的数据传输和能量传输与从应答器到阅读器的数据传输在时间上是交叉进行的，这就是时序法。

1．电感耦合

1）应答器的供电

用电感耦合的时序系统只适合在 135kHz 以下的频率范围内工作。在阅读器线圈和应答器线圈间存在着变压器耦合作用。通过阅读器交变场的作用在应答器线圈中感应的电压被整流，可作为供应电压使用。

为了达到高效传输能量，必须使应答器的谐振频率与阅读器的频率一致，而且还必须实现应答器线圈的高品质因数。所以，应答器含有一个

“片上微调电容器”。该电容器用于补偿谐振频率的容差。

与全双工系统和半双工系统相反，在时序系统中，阅读器的发送器不是连续工作的。在传输过程中传给发送器的能量用于使电容器充电，以存储能量。在充电过程中，应答器的芯片切换到省电或备用模式，从而使接收到的能量几乎完全用于充电电容器的充电。在固定的充电时间结束后，将阅读器的发送器重新断开。

在应答器中存储的能量用于对阅读器发送响应信号。根据所需要的工作电压和芯片的功耗可以计算出充电电容器的最小值：

$$C = \frac{Q}{U} = \frac{I \cdot t}{[V_{max} - V_{min}]}$$

式中：

V_{max} ： V_{min} 工作电压的极限值，不允许超出这个极限值

I ：在工作过程中，芯片的电流消耗

t ：从应答器到阅读器的数据传输所需要的时间

例如：当要求 $I = 5\mu A$，$t = 20ms$，$V_{max} = 4.5V$ 和 $V_{min} = 3.5V$ 时可得出充电电容器的电容量 $C = 100nF$[21]。

2）应答器至阅读器的数据传输

在时序系统中，一个完整的读出周期由两个阶段构成：充电阶段和读出阶段。

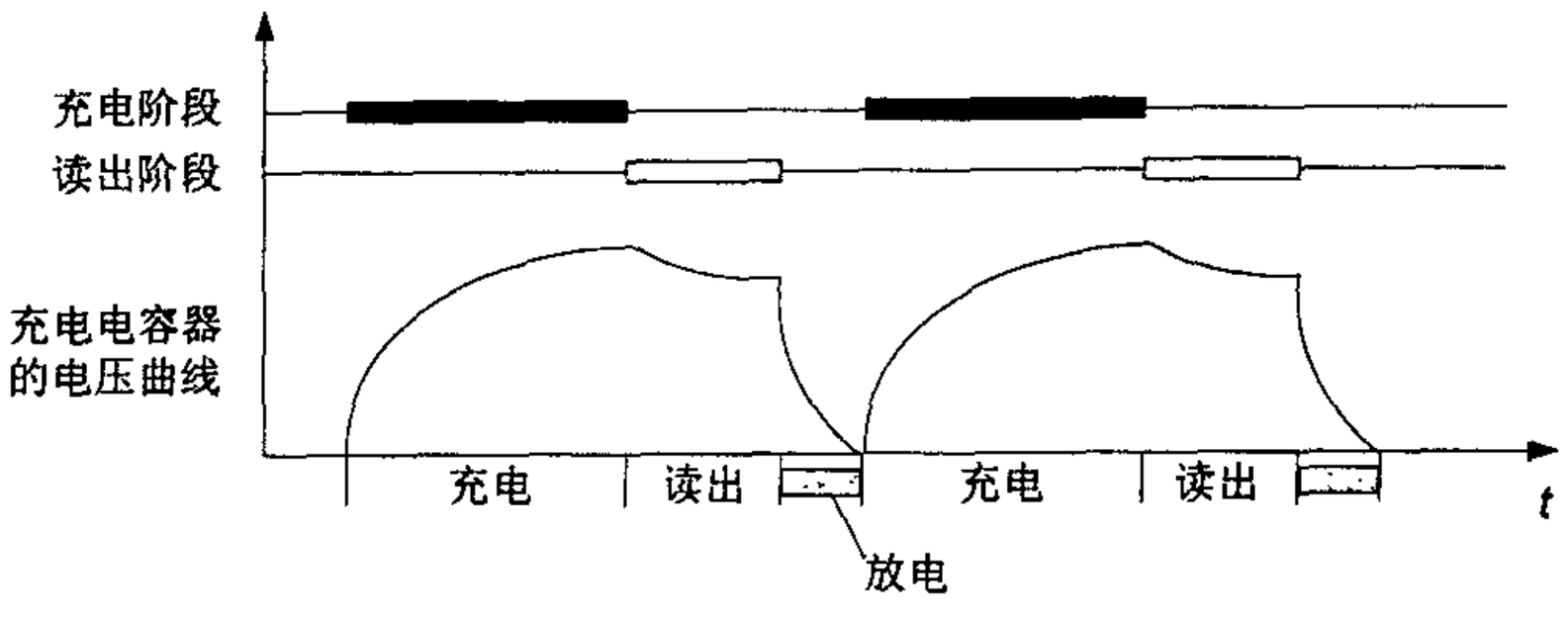


图2.8 电感耦合时序应答器的充电电容器在工作过程中的电压波形

充电阶段的结束是由“脉冲串结束探测器”探测到的。该检测器监视应答器线圈上的电压曲线，并识别阅读器场断开的时刻。随着充电阶段的结束，芯片上的震荡被激活。该振荡器使用由应答器线圈构成的振荡回路

作为决定频率的因素。应答器线圈产生的弱交变磁场，能被阅读器接收。与全双工系统和半双工系统相比，可改善的信号干扰的状况，典型的有20dB。这对时序系统的作用距离产生积极的影响。

为了能调制在无电源供给情况下产生的高频信号，在数据流动的同时，将一个附加的调制电容器与谐振回路并联起来[34]。由此得出的谐振频率的频移键控提供了双频键控（2－FSK）调制。

当所有的数据发送完后，激活放电模式，以便使充电电容完全放电。由此可以保证在下一个充电周期时为完全的电源复位。

2.3.3 全双工、半双工和时序系统的比较

因为在全双工系统中从阅读器到应答器的能量传输与数据的双向传输是同时进行的，所以芯片永远处于工作模式。应答器天线（电流源）与作为负载的芯片（电流消耗）间的功率匹配是最优化的利用所传输的能量的理想途径。然而，如果实现精确的功率匹配，只有电源电压（等于线圈的开路电压）的一半供芯片使用。为了提高供使用的工作电压，只有增大芯片的阻抗（等于负载电阻），而这也意味着功率消耗的降低。

当设计全双工系统时，在功率匹配(即$U_{芯片}=\frac{1}{2}U_0$时的最大功耗$P_{芯片}$)

和电压匹配（即最大电压$U_{芯片}=U_0$时的最小功率$P_{芯片}$）之间必须找到一个折衷方案。

时序系统的情况是完全不同的：充电过程中，芯片处于备用模式或低功耗模式，这意味着芯片好像没有消耗功率。

充电电容器在充电过程开始时已经完全放电。因此，对电压源呈现为很低的负载电阻。在这种情况下，最大电流流入充电电容器，而电压接近于零（等于电流匹配）。随着充电电容器的进一步充电，充电电流按照指数函数下降。当电容器完全充电时，充电电流变为零。充电电容器的状况与应答器线圈的电压匹配状况相符。

时序系统与全双工系统、半双工系统相比，可得出这种情况下芯片能量供应的优点如下：

- 应答器线圈的全部电源电压供芯片工作时用。因此，供使用的工作电压达到相比的全双工和半双工系统的工作电压的两倍。
- 供芯片使用的能量是由充电电容器电容以及充电时间决定的。从理

论上说，这两个可能选择的值是任意大的。对全双工系统和半双工系统来说，芯片的最大功率消耗受功率匹配点（就是说，通过线圈几何图形和场强 H）的限制。

2.3.4 电感耦合射频识别系统的适用频率选择

对一个电感耦合的射频识别系统的频率选择来说，应该考虑到一些供使用的频率范围的特性。所策划的系统工作范围内的可用场强对系统参数有着决定性的影响。因此，应该对这些参数作进一步的试验。此外，也应该考虑带宽、天线线圈的（机械）尺寸和频带的可使用性。

在天线的距离增大时场强的下降起初为 60dB/每 10 倍距离，而在过渡到距离为 $\frac{\lambda}{2\pi}$ 的远场后，场强的下降为 20dB/每 10 倍距离。这种特性对系统工作范围内的可利用场强有着巨大的影响。不论使用什么工作频率，规范 EN300330 规定了距阅读器 10m 时的最大磁场强度[2]。

给定 10m 距离上相同的场强，用较低频带比用较高频带在阅读器的工作范围内（例如 0~10cm）能达到的有用场强更高。在小于 135kHz 时，情况甚至更加有利，首先由于容许的场强极限值远高于 1MHz 以上的频带的容许值，其次，60dB 的增加立即见效，因为在这个频带时近场至少扩展到 350m。

如果在不同频率时，用相同的磁场强度去测量电感耦合系统的作用距离，就可以发现在 100MHz 左右的频带的作用距离最大。其原因在于 $U_{ind} \sim \omega$ 的比例关系。在大约 10MHz 的较高频率时，功率传输效率明显地大于 135kHz 以下的频率的效率。

然而，这种效应由于 135kHz 的容许场强而得到补偿，以致在实践中两种频率范围的射频识别系统的作用距离大体相同。在 10MHz 以上时，应答器振荡回路的 L/C 关系变得越来越不利，以致在这个频率范围内的作用距离开始减少。

- **频率范围 13.56MHz：** 频率范围 13.553~13.567 处于短波范围中间。在这个频率范围内的传播条件允许昼夜横贯大陆联系。这个频率范围的使用者是不同类别的无线电服务机构，例如新闻机构和电信机构(PTP)。这也是射频 IC 卡国际标准所指定的频率范围[47]。

第三章 IC卡数据结构与安全性

3.1 IC卡数据的逻辑结构

3.1.1 数据对象的编码

在IC卡系统应用中，IC卡与终端之间进行信息的交换和处理时，需要对数据进行编码，以实现对数据的上下文解释。IC卡的数据结构采用BER-TLV的基本规则编码，在这种规则中，数据对象由2~3个连续字段组成[20]。

- 标记字段T由一个以上的连续字节组成。它对类别、类型与编号进行编码，一般用1~2个字节来编码，ISO/IEC7816规定不用‘00’或‘FF’作为标记T之值。
- 长度字段L由一个以上的连续字节组成，它对长度（整数）编码，一般使用1~3个字节。
- 值段V位数据对象的编码值，若L=00，就没有值段，否则，值段长度的字节数，即为L之值。

BER-TLV数据对象可分为基元数据对象与结构数据对象两类，前者的值段仅含有一个数据元，后者的值段则含有一个以上的基元数据对象。一个结构数据对象的值段叫做一个属性模板或简称为模板。

这里所说得BER-TLV数据对象的具体编码规定如下[20]：

（1）标记字段

BER-TLV数据对象标志字段第一字节的结构如表3.1所示。

《EMV规范》对BER-TLV数据对象标记字段的编码具体规定为：

- ISO/IEC7816规定的应用类模板使用“61”和“6F”。
- 《EMV规范》规定的应用类模板使用“70”至“77”，按照该规范这是一个应用制定的定义使用。
- 数据前后关系指定类的数据对象按其出现的属性模板的数据前后关系来规定。
- “81”至“9E”和“9F01”至“9F4F”的数据前后关系指定的基元数据对象的编码保留为《EMV规范》所使用。

• “9F51”至“9F7F”的数据前后关系指定类的基元数据对象的编码保留给支付系统使用。

b8	B7	b6	b5	b4	b3	b2	b1	含义
0	0							通用类
0	1							应用类
1	0							数据前后关系指定类
1	1							专用类
		0						基元数据对象
		1						结构数据对象
			1	1	1	1	1	见后接字节
			大于 0 的任何值					标记号
			0	0	0	0	0	未用

表 3.1　BER-TLV 标记字段第一字节的结构

• 专用类的基元和结构数据对象的编码留给发卡方自定。

装在模板“76”的数据前后关系指定类功能对象的编码与《EMV 规范》规定的数据前后关系指定类数据对象的编码是重叠的。

按照 ISO/IEC8825，表 3.2 规定了在标记号大于 31 以后的 BER-TLV 标记字节的编码规则。

b8	B7	b6	b5	b4	b3	b2	b1	含义
1								后跟另一个字节
0								最后的标记字节
	大于 0 的任何值							标记号（部分）

表 3.2　BER-TLV 标记字段后继字节的结构

（2）长度字段

长度字段的编码如下：

短格式时，长度字段只有一个字节，此时该字节的最高位 b_8=0，b_7~b_1

表示值段的字节数，其范围为 1~127。

长格式时，长度字段含有一个引导字节，其最高位 b_8=1，而 b_7~b_1 则表示长度字段的后继字节数。后继字节的内容为一整数，代表值段中的字节数。在 APDU（应用协议数据单元）中的任何长度（最长为 65，536 个字节），均可用三个字节来编码。

（3）值段

数据源是基元 BER-TLV 数据对象的值段 V，数据源是得到标识符（标记）的最小数据字段。

基元数据对象和结构数据对象的结构如图所示：

A. 基元BER-TLV数据对象（数据元）

标记（T）	长度（L）	值（V）

B. 结构BER-TLV 数据对象

标记（T）	长度（L）	基元BER-TLV数据对象1	……	基元BER-TLV数据对象n

图3.1 数据对象的结构

3.1.2 数据对象的传送和检索

1．数据对象的传送

IC 卡中的数据被装在数据对象之中，这些数据对象可以存储在文件的记录内，IC 卡与终端交换的数据元可以被装在数据对象内。

在一个命令报文的数据字段中，从终端传送到 IC 卡的数据元不使用标记与长度，所传递的只是每个数据对象的值段（换言之，是一数据元）在一个命令报文的数据字段中，若必须有一个以上的数据元从终端传送到 IC 卡，则这些数据元的连接是无分界符的。

从 IC 卡传送至终端的数据元必须装在响应报文数据字段具有标记与长度的模板之中。

含有一个或一个以上的基元数据对象或结构数据对象的模板称为纪录。

数据对象在记录中的变换由发卡方自定。

2．数据对象的类别

在数据对象的编码字节中，已经对数据对象的类别作了规定，同时给出了标志与编码的规定。其中关于标记的定义遵照了 ISO/IEC8825 和

ISO/IEC7816 标准系列，并且适合于和《EMV 规范》相一致的应用。

3．数据对象的检索[8]

送至 IC 卡或从 IC 卡回送的不需 IC 卡解释的数据元，必须装在一个记录的数据对象之中。而送到 IC 卡或从 IC 卡回送的作为计算的输入或结果的数据元，必须按各自命令-响应的应用协议数据单元（APDU）的格式装在命令或响应报文之中。从 IC 卡回送的数据元及其所包含的可由 IC 卡解释的数据应装在数据对象之中。

3.1.3 文件

1．文件组织

在处理交换行为的行业内部命令时，在接口处所见到的数据的逻辑结构如上节所述是按 BER-TLV 规则编码的。并且，按照基元数据对象、结构数据对象、记录和文件的层次结构存储在 IC 卡中。为了交易处理的方便（可靠、快捷和节省存储空间），特别是便于实现在一张卡中支持多个应用，ISO/IEC 7816 还规定了文件的组织，这里允许支持两类文件[20]：

— 专用文件（DF）

— 基本文件（EF）

IC 卡中的数据的逻辑组织包含了如下的层次结构的专用文件。

— 在根部的 DF 称为主文件（MF）。MF 是强制性的。

— 其他的 DF 是可选的。

规定了两种 EF 文件，它们是：

— 内部基本文件：用于存储由 IC 卡解释的数据，即那些为了管理和控制的目的，由 IC 卡分析和使用的数据。

— 工作文件：用于存储不由 IC 卡解释的数据，即那些在 IC 卡之外应用的数据。

符合《EMV 规范》的应用文件组织称为“支付系统应用”（PSA）。在一个 IC 卡中，可以有多个应用。所以，除 PSA 外，尚可存在有符合 ISO/IEC 7816-4 但不符合《EMV 规范》的应用文件组织。

在 IC 卡中通向 PSA 文件集的路径是由直接选择的支付系统环境（PSE）来启动的。PSE 的成功选择就进入了 PSA。

从终端来看 PSA 文件及犹如一个树结构，可通过树形的目录组织来访问。树的每一分枝是一个应用定义文件（ADF），一个 ADF 是一个或一个以上的应用基本文件（AEF）的入口点，ADF 及其有关的数据文件是

在树的同一分枝上。

— 应用定义文件 ADF 及其树形结构：

. 能使数据文件附属在一个应用上；

. 确保各应用之间分开；

. 通过对它的选择，容许访问该应用的逻辑组织。

在终端看来，ADF 是个只含有数据对象的文件，该数据对象被装在它的文件控制信息 FCI 中。

— 应用基本文件 AEF。

AEF 含有一个或一个以上的按 BER-TLV 编码的基元数据对象，他们又归类到结构的模板（记录）之中。选择应用后，AEF 仅按短文件标识符 SFI 来引用。

数据文件是由用其记录号地址的记录序列所组成，由 SFI 引用的文件只含不被 IC 卡解释的数据，换言之，它们是工作文件。这种文件被规定为线性的，也可以是可变线性结构，由发卡方自定。

— 文件在 ISO/IEC7816-4 文件组织上的变换

以下在 ISO/IEC 7816-4 上的变换适用于：

. 如 ISO/IEC 7816-4 所规定，含有一个 FCI 的专用文件（DF）被变换到 ADF 上，它可以提供对基本文件 EF 和专用文件 DF 的访问。支付卡上的最高层 DF 是主文件 MF。

. 如 ISO/IEC 7816-4 所规定，含有一组记录的 EF 被变换到 AEF 上，EF 决不用作另一个文件的入口点。

如果 DF 是被嵌入的，则对其所附属的 EF 的检索，对于《EMV 规范》来说是透明的。

2. 目录组织

IC 卡必须保持一个目录组织，以列出在 PSE（支付系统环境）范围内的应用，这些应用在服务过程中要通过目录进行选择，目录由一个强制性的支付系统目录文件（DIR 文件）与可选的附加目录组成，二者皆有目录定义文件 DDF 所引用。

采用树形的目录组织，使得可用应用标识符 AID 对此应用进行检索，或选用 AID 的头几个字节作为 DDF 名对一组应用进行检索。

IC 卡中不属于支付系统目录是可选的，对这些可能存在的目录，没有数量限制的规定。每个这样的目录，由包含在每个 DDF 的 FCI（文件

控制信息）中的 SFI（短文件标识符）数据对象目录来定位。

3．对文件的访问

当一个文件若不能被隐含地选择时，它应当至少用下述方法之一被选择：

— 由名称访问：在支付卡中任意 ADF 或 DDF 都应有对应于 AID 或 AID 的头几个字节的 DF 名来访问，每个 DF 名在支付卡内必须是唯一的。

— 由文件标识符访问：文件标识符用两个字节编码。MF 的文件标识符规定为‘3F00’、‘FFFF’和‘3FFF’都是 RFU 值，为了能毫无疑义地用标识符选择每一文件，所有的 EF 和 DF 只要位于同一个 DF 之下都应有不同的标识符。

— 由路径访问：任何一个文件都应当能用路径（文件标识符的连接）进行访问。路径由 MF 或现行的 DF 的标识符开始，终止于被访问文件本身的标识符，在此二标识符之间则是可能有的相继的父 DF，标识符的顺序总是从父到子。若不知现行 DF 的标识符，则可以‘3FFF’作为路径的起点，路径容许无疑义地由 MF 或现行 DF 访问任一文件。

— 由 SFI 访问：SFI 可用于对 AEF 的选择，SFI 用 5 位来编码，范围为 1~30。SFI=0 用来表示对现行选择的 EF 的访问。《EMV 规范》中对 SFI 的编码之规定如下：

值	1~10	11~20	21~30
含义	EMV 规范管理的范围	由支付系统规定	由发卡方规定

在一个应用中，SFI 必须是唯一的，它不能当作路径或文件标识符来使用。

3.1.4 MIFARE®— 应用目录

本文所主要介绍的为非接触式 IC 卡，而作为非接触式 IC 卡中的应用最为广泛的 MIFARE®系列 IC 卡不能不对其进行介绍。由飞利浦公司开发的 MIFARE®系列非接触式 IC 卡已经成为了 TYPE A 形卡片的一种应用型标准，在全世界有多个公司生产 MIFARE®系列的非接触式 IC 卡。

MIFARE®系列 IC 卡的存储器被分成 16 个独立段，称之为扇区。每个扇区用两个不同密钥（分级结构）防止非认可的访问。在它自己的访问存储器中可以对两个密钥授予不同访问权。这样 16 种彼此独立的应用可由装入 IC 卡的秘密密钥分别予以保护。没有秘密密钥就没有应用可以读出，甚至不能检查或识别。所以，连 IC 卡中存有哪些应用也无法断定。

假设发行非接触式的城市卡，人们可以用这种 IC 卡来使用城市的服务，而这些只占用卡上可用存储器的一小部分。卡上剩余的存储单元可以由其他服务提供者为他们自己的应用所使用。但是，现在不能查明卡上的许多应用中那种是当前可用的，因为每一种应用的阅读器只能访问它自己的扇区，还要有正确的密钥。

为了回避这个问题，飞利浦公司采用了 MIFARE®—智能卡应用目录（MAD），如图 3.2 所示[45]。

扇区 0 的字组 1 和 2 是为 MAD 保留的，留有 32 字节供应用目录使用。每 2 字节构成一个指针，ID1 至 ID$F，指向剩余的 15 个扇区之一。读出指针的内容，则读出 2 个字节：功能组和应用代码。后者可用来在一外部数据库中查找应用。即使要查找的应用未在受查访的数据库中注册，仍能从功能组得到大概的分类，例如“航空线”、“铁路服务”、“公交服务”、“城市卡服务”、“停车场”等等。

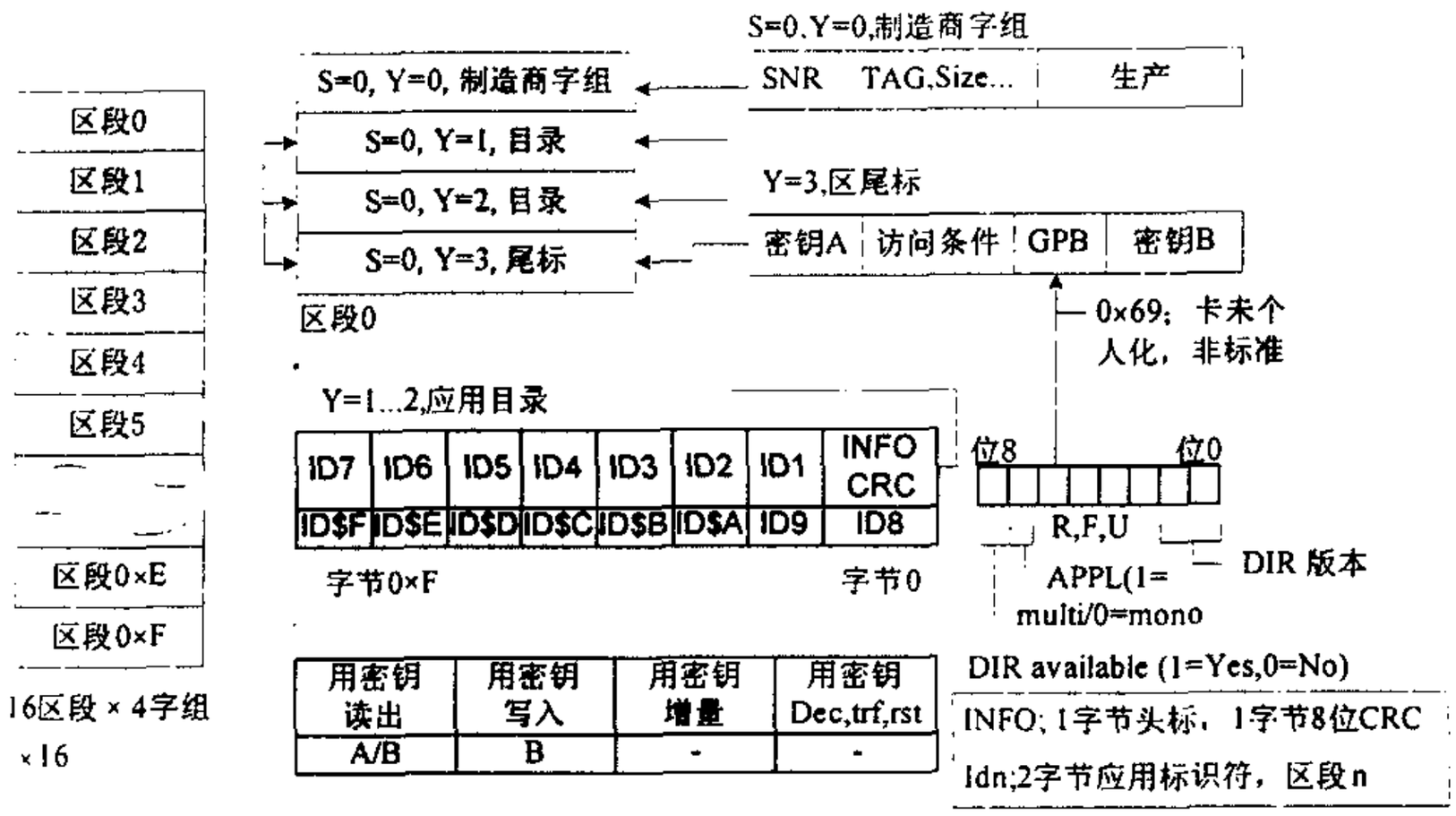


图3.2 MIFARE应用指南的数据结构由15个指针组成（ID1至ID$F），他们指向后继的区段

每个应用分配了一个唯一的识别号，由功能组代码和应用代码组成。可以从 Gnaz 的 Philips Semiconductors Gratkorn（Mikron）的 MIFARE®技术开发者那里申请识别号。

如果功能组被置为 00，则是个管理代码，被用于管理空白的或备用的扇区。

扇区 0 本身不需要 ID 指针，因为 MAD 本身被存储在扇区 0。因此空下的 2 个字节用于存储 Info 字节和 CRC，后者用于校验 MAD 的结构错误。在 Info 字节的空 4 位中，可以存储一个备注，给出卡发行者的扇区 ID。这样即使在智能卡上记录了多于一个的应用，阅读器也能判定卡的发行者。

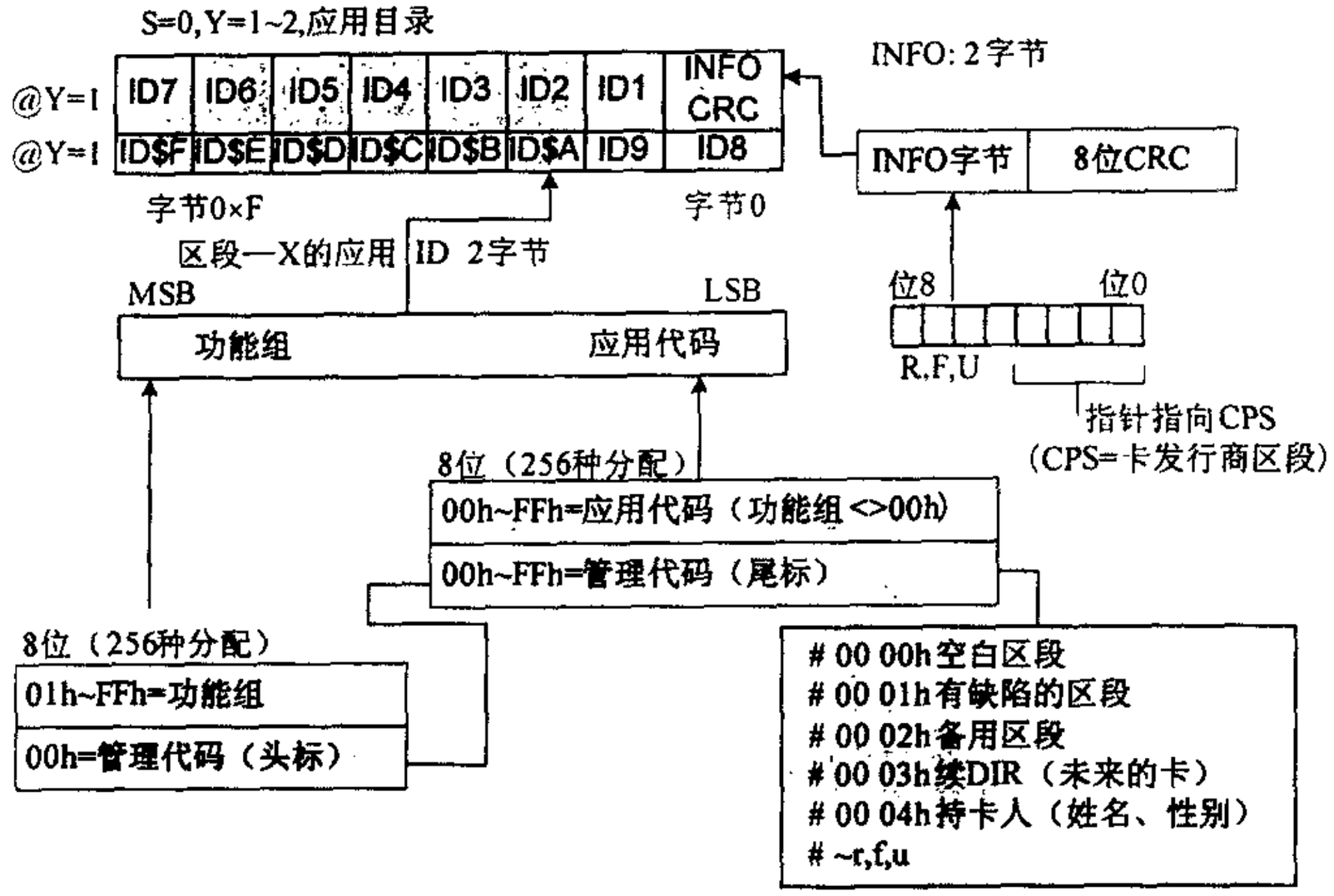


图3.3　MIFARE应用目录的数据结构：从15个指针（ID1至ID$F）的内容可以查明在每个区段种分配的应用

另一个特点是 MAD 的密码管理。读取 MAD 所需的密钥 A 是已经发行了的，记录进一步的应用需要密钥 B，则由卡发行商管理登记。这就是说，另外的服务提供者对卡的共同利用只有在共同利用契约缔结和发行了相配的密钥后才是可能的。

3.2　IC 卡的安全性

从前面提到的 IC 卡的历史中可以看到，IC 卡从诞生到现在的发展是非常迅速的。在如今磁卡技术非常成熟和广泛使用的境况下，IC 卡之所以备受重视，进而后来居上的一个重要原因就是它有着较磁卡要好得多的安全性和可靠性。

3.2.1 密码系统

所有的密码系统都按相同的基本方式工作：把一个原本的消息（称之为明文）通过加密算法和加密密钥转换成编码的消息（密文）。它仅能被解密算法和解密密钥所译码。秘密通常保留在密钥上，不在算法上，因为使用标准的算法有着明显的商业价值。事实上，密码员是在最不利情况的假设下工作的。即整个加密机制为所有多方面所了解（基尔霍夫假设）[12]。

密码系统可分为不同的两类，即保密密钥系统和公开密钥系统[10]。实际上，二者都要使用保密的密钥。

保密密钥的关键之点在于算法是完全可逆的（亦即对称的），所以又被称为对称密钥系统。如果对密码电文执行加密操作，将再次获得原本的普通电文。

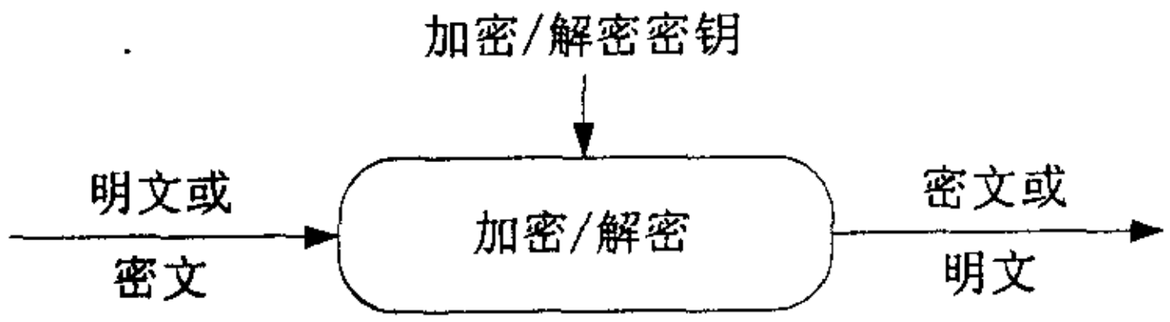


图3.4 保密密钥系统的工作方式

保密密钥系统的核心是密钥，它有着高度的机密性。问题在于如果一个人知道了密钥之后，他就可以破译该密钥所加密的消息，而系统无法查明该密钥是这个人自己的还是非法得到的。另外，当有着许多对的发送者和接收者时，由于每一对之间都需要一个单独的相互同意的密钥，这就成了一个十分蹩脚的不实际的问题了。因为密钥的数量可能达到人数的平方的数量级。

由此，人们引入了非对称密码系统的概念，即加密和解密算法是不同的。使密码电文再次通过加密系统时，不能产生出原本的消息，因而系统是不对称的。在这种情况下，需用两个不同的密钥，一个用于加密，一个用于解密。这些密钥有着数学上的联系，并可能设计出一种算法使得加密密钥可以公开，然而用这种方法确定的解密密钥则不能公开。

具有这种性能的密码系统称为公开密钥系统。在这种系统中要发送一则加密的消息时，发送者应先从一张公开的表中查到接收者的加密密钥，并用此密钥对消息加密。然后发送者可用不保密的通讯方法来发送这份密

文。接收者则用他保密的解密密钥予以译解。

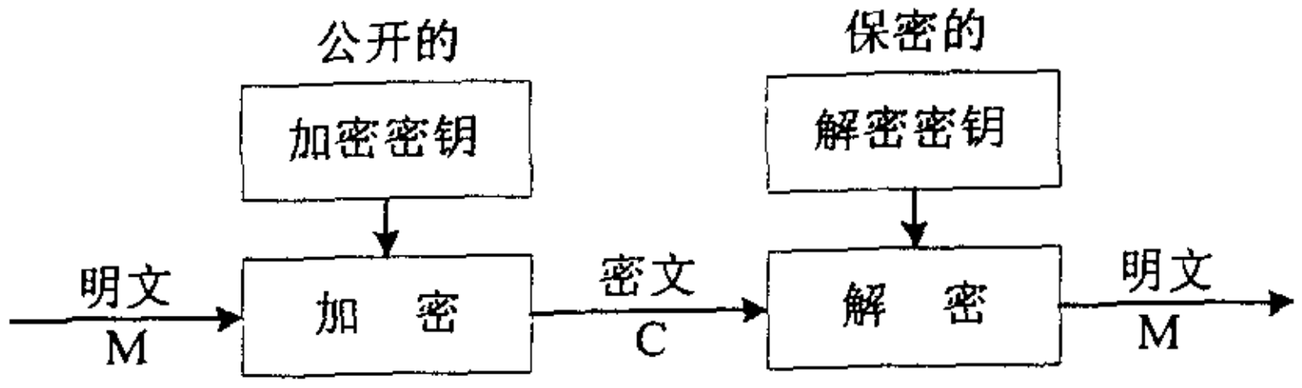


图3.5 公开密钥系统的工作方式

公开密钥有两个非常重要的优点，首先是大大地简化了密钥的分布和管理，因为每个人只需记住它自己的解密密钥就可以了。其次是提供了实现“电子签名”的可能性，这是一种在应用中，诸如家庭银行和电子邮件等特别重要的性能。

在IC卡的保密系统中，目前采用得最多的是保密密钥系统。而对于公开密钥系统的使用由于在硬件上的限制，目前的使用还非常地少。然而，随着CPU卡的不断发展，在将来的智能卡系统中将会更多地采用公开密钥系统以便实现电子签名在IC卡中的使用[19]。下面将介绍两种加密算法，这是在智能IC卡中广泛应用的两种算法。

3.2.2 加密算法

1．DES算法：

DES算法是一种对称密钥体制的加密方法，它的全称是Data Encryption Standard。是IBM公司于1975年研究成功并公开发表的，这也开创了公开全部算法的先例。

DES算法是把64位的明文输入块变换为64位的密文输出块，它所使用的密钥也是64位的，其中8位为奇偶校验位。要加密的一组数据先经过初始置换IP的处理，然后通过一系列的迭代运算，(最后经过IP的逆置换 IP^{-1} 给出加密的结果。整个算法的流程如图3.6所示，其中 k_i（i=1~16）是初始密钥K经分解、移位后产生的48位长的子密钥。可见，与密钥有关的算法包括子密钥的生成和密码函数f。

（1）初始置换IP[13]

IP的功能是将输入的64位数据块按位重新组合，并把输出分为 L_0、R_0 两部分，每部分各长32位，如上表所示。即将输入的第58位换至第1位，第50位换至第2位...最后一位是原来的第7位。L_0 和 R_0 则是换位

输出后划分的两部分，L_0是输出结果的左边 32 位，R_0是右边的 32 位。如果令置换前的输入值为 $b_1b_2...b_{64}$，则经过初始置换后的结果为：

$$L_0=b_{58}b_{50}...b_8 \qquad R_0=b_{57}b_{49}...b_7$$

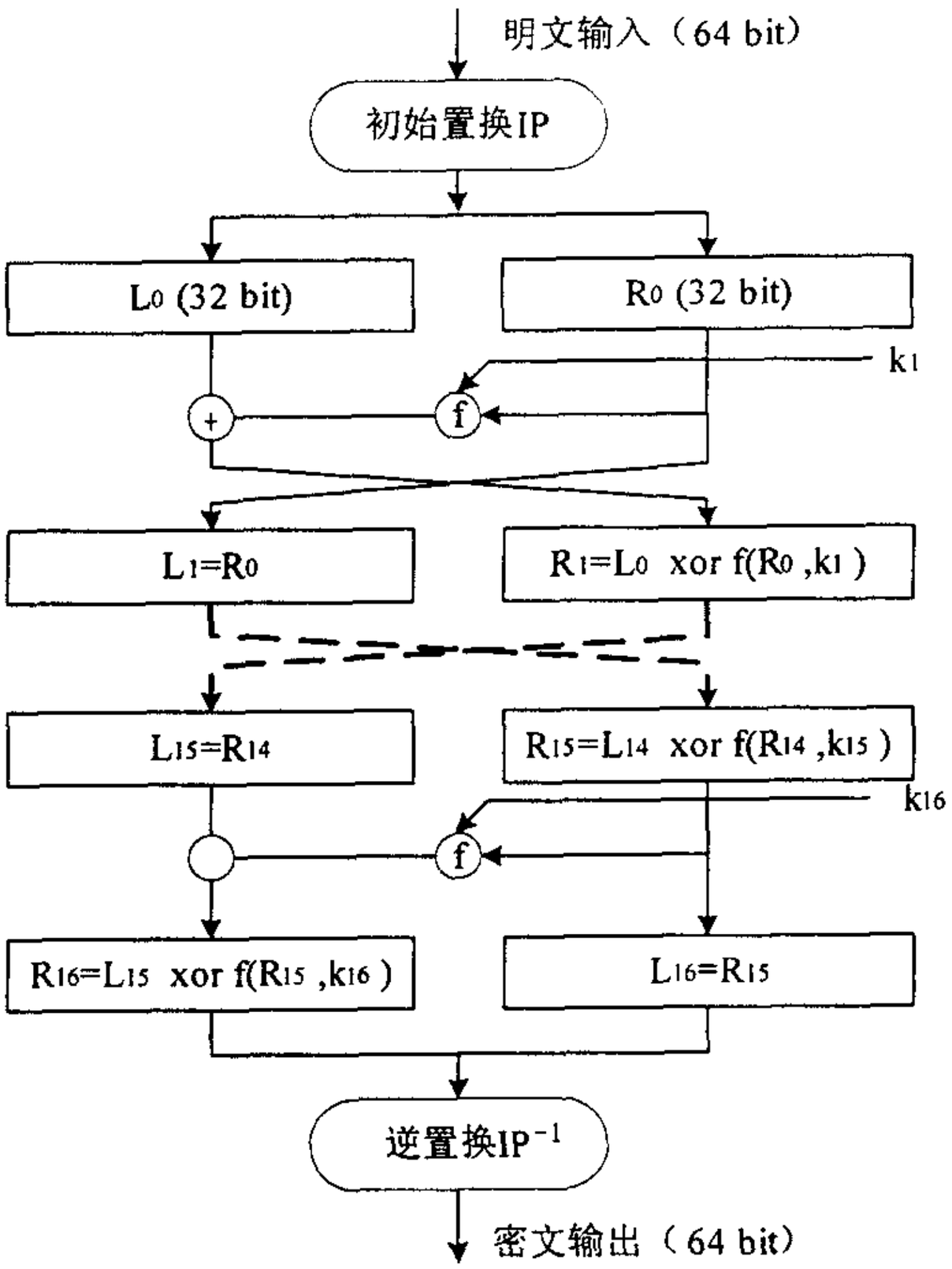


图3.6 DES算法 [13]

（2）16 次迭代

接下来就是迭代过程，将 R_0与子密钥 k_1经密码函数 f 的运算得到 $f(R_0, k_1)$，与 L_0按位模 2 加得到 R_1，将 R_0作为 L_1，就是完成了第一次迭代，以此类推，第 i 次的迭代可以表示为：

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$$

在迭代过程中，最重要的部分是函数 f。f 的结构如图 3.7 所示。它的功能是利用放大换位表 E 将 32 位的 R_{i-1} 扩展至 48 位，与子密钥 k 按位模 2 加后，把结果分为 8 个 6 位长的数据块，在分别经选择函数 S_1，S_2，…，S_8 的变换。产生 8 个 4 位长的块，合为 32 位，最后经过单纯换位 P 得到输出。

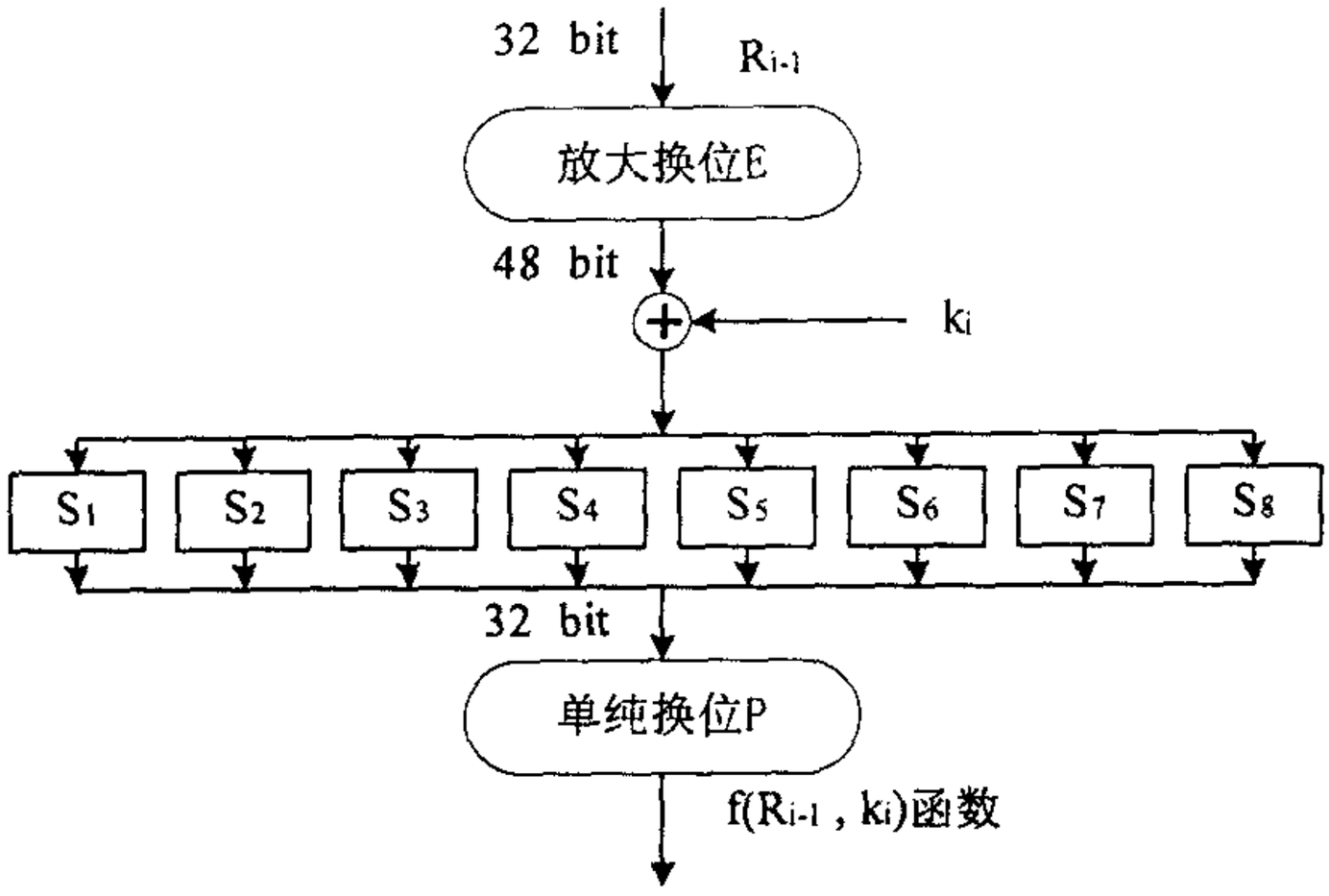


图3.7　f(Ri-1 , ki)函数

（3）逆置换 IP^{-1}

经过 16 次迭代运算后，得到 $R_{16}L_{16}$，将之作为输入，进行逆置换 IP^{-1}，即得到密文。IP^{-1} 完成的功能正好是 IP 的逆过程。

（4）子密钥的生成

密钥 K 本身为 64 位，但其中第 8，16，24，…，64 位是奇偶校验位，所以 K 实质只有 56 位。将这 56 位的数据经过选择换位 PC-1 后产生的结果分为两部分 C_0、D_0，分别是左、右各 28 位，然后分别经过循环左移位，得到 C_1、D_1，合并后，再经缩小换位 PC-2，即得到子密钥 k_1，依此类推可以产生 k_2，k_3，…，k_{16}。

2．多重 DES 加密

对明文进行多次加密称之为“多重加密”，用同一算法和同一密钥对一明文加密两次并不影响强力攻击的复杂性，增加安全性需要多重密钥。

三重加密是较好的方法，它用两个密钥对明文加密/解密 3 次。发送

者先用第一个密钥对明文加密，然后用第二个密钥解密，最后用第一个密钥加密；接收者用第一个密钥解密，用第二个密钥加密，最后用第一个密钥解密。

$$C = E_{k1}(D_{k2}(E_{k1}(P)))$$
$$P = D_{k1}(E_{k2}(D_{k1}(C)))$$

三重 DES（Triple DES）加密算法的加/解密过程如图 3.8 所示[4]：

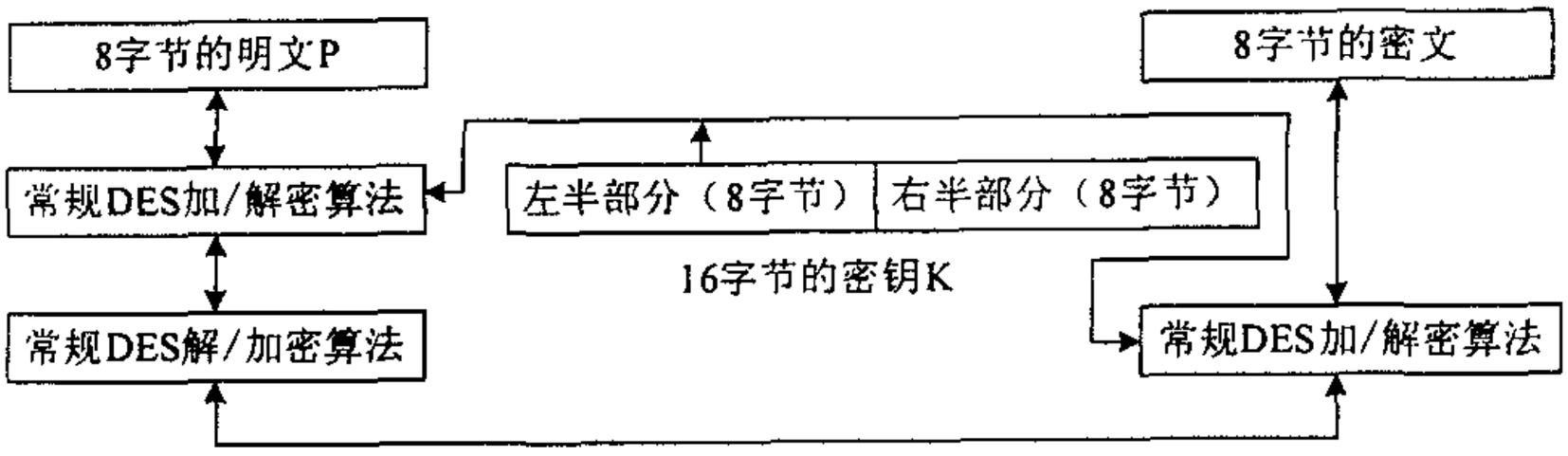


图3.8　三重DES数据加密算法

对称密码体制的密钥使用了一段时间以后就需要更换，加密方需通过某种秘密渠道把新密钥传送给解密方。在传递过程中，密钥容易泄漏。另外，由于对称密码体制的加密密钥和解密密钥是相同的，所以当在智能卡中采用 DES 算法，信息的收发方对信息内容及发送原点产生争执时，DES 算法就显得无能为力了。在下面将介绍非对称密码体制算法，可以解决上述问题。

3．RSA 算法

RSA 算法是由 Rivest、Shamir 和 Adleman 三个人提出来的，从提出到现在已经经历了十多个年头，经受了各种攻击的考验，被认为是目前最优秀的非对称密码方案之一。

RSA 算法是一种分组密码算法，它以数论为基础，其安全性是建立在大整数的素数因子分解的困难性上的，现在数学上还没有一种有效的算法来解决这类的问题。要建立一个 RSA 密码系统，首先任意选取两个大素数 p、q，计算乘积 n：

$$n = p \cdot q$$

并得到 Euler 函数：

$$\phi(n) = (p-1)(q-1)$$

然后，任意选择一个与ϕ(n)互素的整数 e 作为加密密钥，再根据 e 求出解

密密钥 d，d 满足：

$$de \equiv 1 \bmod \phi(n)$$

事实上，加密密钥 e 和解密密钥 d 在功能上是完全可以互换的，因此在生成 e、d 时，不论先假设哪一个，再由他去求另一个都是可以的。在这些参数（p、q、n、$\phi(n)$、e、d）中，p、q、$\phi(n)$、d 是保密的，n、e 则是公开的。在后面的计算中，p 和 q 已不再需要，可以舍弃，但决不能泄露。有了这些参数，就能进行加密和解密运算了。

加密之前，先将明文（以 m 表示）数字化，把用二进制数据表示的明文分成长度小于 log n 位的明文块，以确保每个明文块不超过 n。把明文 m 加密的过程是：

$$c \equiv E(m) = m^e \bmod n$$

式中 c 即为密文。

解密的过程则是：

$$m \equiv D(c) = c^d \bmod n$$

利用 Euler 定理可以证明该加密/解密过程的一致性。

3.2.3 IC 卡数据的安全性

IC 卡的安全系统应该能够对下述单项的攻击予以防范：

- 为了复制与/或改变数据，未经授权地读出数据载体。
- 将外来的数据载体置入某个阅读器的询问范围内，企图得到非授权的访问。
- 为了假冒真正的数据载体，窃听无线电通信（射频通信）并重放数据（“重放和欺诈”）

所以在 IC 卡的使用过程中，应该对数据载体（IC 卡）和阅读终端进行相互的认证和鉴别。

1．PIN 鉴别

个人鉴别从持卡人键入 PIN 开始，PIN 经安全通道从终端传送到 IC 卡上，与秘密存储在 IC 卡上的 PIN 基准值（称为个人验证值 PVV：Personal Verification Value）相比较，若两者相符，则证明持卡人是合法用户，否则就是非法用户。

2．对称密钥系统的鉴别

在对称密钥系统中，所有应答器（IC 卡）和阅读器（终端）构成了某项应用的一部分，具有相同的密钥 K（对称过程）。当某个应答器首先

进入阅读询问范围时，它无法断定参与通信的双方是否属于同一个应用。从阅读器看，需要防止伪造数据的假冒。另一方面，应答器同样需要防止存储数据未被认可的读出或重写[25]。

互相鉴别的过程从阅读器发送“查询口令”的命令给应答器开始。于是在应答器中产生一随机数 R_A，并回送给阅读器（应答→口令回令过程）。阅读器则产生一随机数 R_B。使用共同的密钥 K 和共同的密码算法 e_k，阅读器算出一个加密的数据块[权标（Token）1]。它包含了两个随机数及附加的控制数据，并将此数据块发送给应答器。

$$\text{Token 1}=e_k(R_B \| R_A \| ID_A \| \text{ 电文 1})$$

在应答器中，收到的 Token 1 被译码，并将从明文中取得的随机数 R_A' 与原先发送的随机数 R_A 相比较。如果两数一致，则应答器已确认两个公有的密钥是一致的。应答器中另行产生一个随机数 R_{A2}，并用以计算出一加密的数据块（Token 2），其中也包含有 R_B 和控制数据。Token 2 由应答器发送给阅读器。

$$\text{Token 2}=e_k(R_{A2} \| R_B \| \text{ 电文 2})$$

阅读器将 Token 2 译码，检察原先发送的 R_B 与刚收到的 R_B' 是否一致。如果两随机数一致，则阅读器方也证明了两个共有的密钥是一致的。于是，应答器和阅读器均已查实属于共同的系统，双方更进一步的通信是合法的。如图 3.9 示：

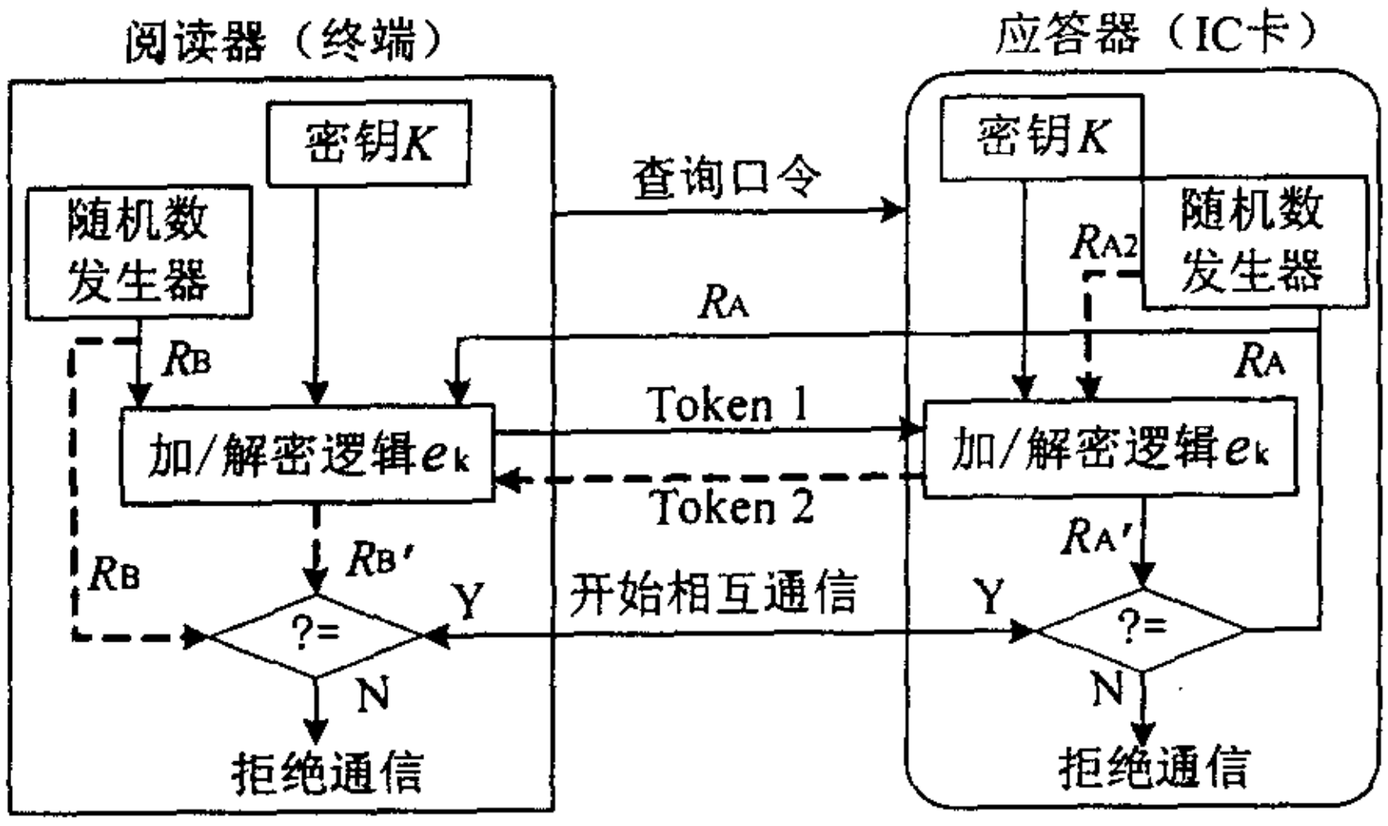


图3.9 阅读器和应答器相互鉴别的过程

相互鉴别的方法具有如下的好处：

- 密钥从不经空间传输，而只传输加密的随机数。
- 总是两个随机数同时加密。排除了为计算密钥用 R_A 执行逆变换以获取 Token 1 的可能性。
- 可以使用任意算法对权标加密。
- 通过严格使用来自两个独立来源（阅读器、应答器）的随机数，使为了在较后的日期重播（回放攻击）而记录鉴别序列的方法必然失败。
- 从产生的随机数可以算出随机的密钥（会话密钥），以便加密保护后继传输的数据。

3．导出密钥的鉴别

上面介绍的鉴别方法的一个缺点是：所有属于同一应用的应答器都使用相同的密钥 K 来保护。这对于具有大量应答器的应用来说是一种潜在的危险源。因为，这些应答器以不可控制的数量而为每个人易于取得。必须考虑到应答器的密钥可能以小概率被揭露，如果这种情况发生了，则上述过程将整个被公开控制。

对所述鉴别过程的主要改进是：每个应答器用不同的密钥来保护。为此，在应答器生产过程中读出它的序列号（ID）。用加密算法和主控密钥 K_M 计算（导出）密钥 K_X。而应答器就这样被初始化。每个应答器因此接受了一个与自己的识别号和主控密钥 K_M 相关联的密钥。

互相鉴别开始于阅读器请求应答器的识别号。当阅读器接收到应答器送过来的识别号后，再用主控密钥 K_M 和识别号一起计算出导出密钥 K_X。然后再利用 K_X 实现相互鉴别的过程。这意味着主控密钥 K_M 决不能读出。

4．加密的数据传输

数据在传输中可能会受到攻击者的攻击，这个攻击可能表现为试图通过窃听传输线路以发现秘密信息而达到非法的目的。或者表现为试图操纵传输数据并为了其个人利益而修改它[14][16]。

加密过程用来防止主动和被动攻击。为此，传送数据（明文）可在传输前改变（加密），使隐藏的攻击者不能推断出信息的真实内容。

（1）流密码

每一步都用不同的函数把明文的字符序列变换为密文序列的加密算法，称为序列密码术或流密码术[35]。流密码术的理想实现方法是所谓的“一次插入”（one time pad）法，也因发明人而称“Vernam 密码术”[39]。

加密数据传输前，这个方法要产生一个随机密钥 K。而且这个密钥对双方均适用。密钥序列与明文序列通过符号相加或用“XOR”选通而连结起来。作为密钥使用的随机序列的长度至少必须与要加密的信息长度相等，因为与明文相比特别短的密钥的周期重复，有可能进行密码分析从而导致对传输线路的攻击。此外，密码只能使用一次，这意味着为了安全的分配密钥需要极高的安全水平。然而，对射频 IC 卡来说，这种形式的流密码是完全不适用的。

为了克服密钥的产生和分配问题，系统应按照“一次插入”原则创建流密码，而使用所谓的伪随机数序列来取代真正的随机数序列，伪随机序列用伪随机数发生器产生。

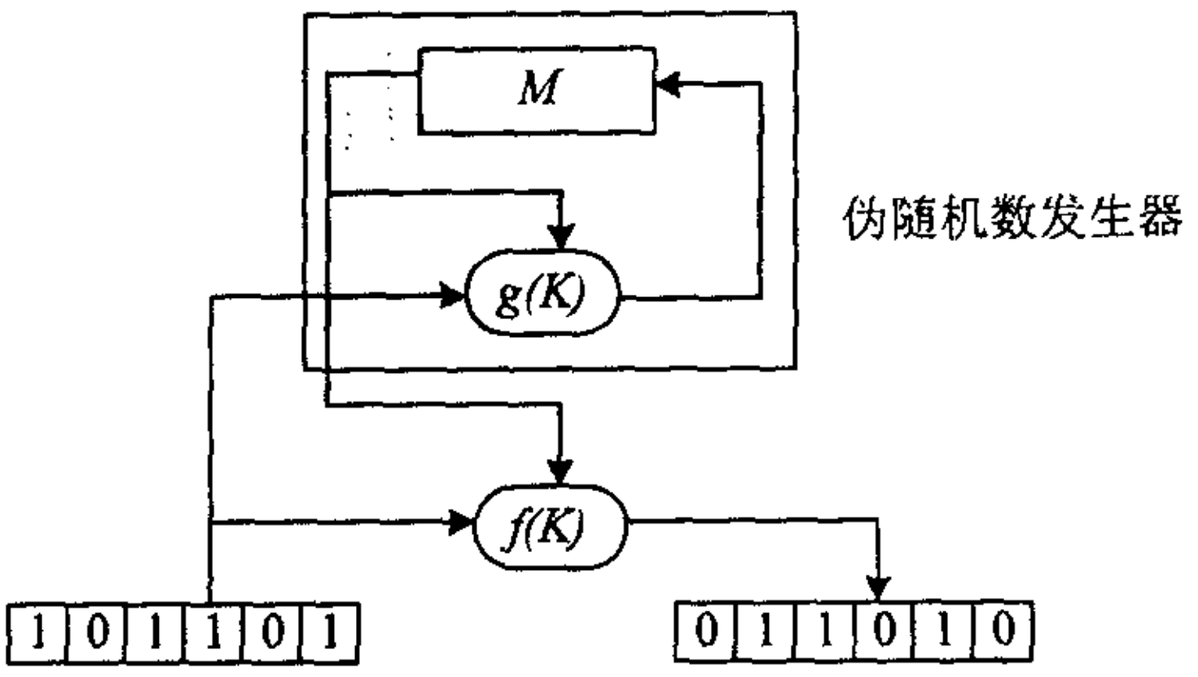


图3.10　用伪随机数发生器产生可靠密钥的原理

图 3.10 所示为使用伪随机发生器的序列密钥的基本原理：由于序列密码的加密函数可以随着每个符号（随机的）改变，此函数不仅应依赖于当前输入的符号，而且还应当依赖于附加的特性，即其内部状态 M。内部状态 M 在每一加密步骤后随状态变换函数 $g(K)$而改变。为随机数发生器由部件 M 和 $g(K)$构成。密文的安全性主要取决于内部状态 M 的数量和变换函数 $g(K)$的复杂性。对序列密码的研究主要是对伪随机数发生器的分析。

另一方面，加密函数 $f(K)$本身通常是很简单的，可能仅包含了加法或“XOR”逻辑门[36]。

第四章　非接触式（射频）IC 卡

非接触式 IC 卡是射频识别技术和 IC 卡技术相互结合的产物，最近几年的发展迅速，推动了 IC 卡应用领域的扩大。相较于接触式 IC 卡而言，避免了卡和阅读器之间的相互接触，从而方便了卡的使用。在实际应用中体现出使用方便、交易速度快、便于维护和卡片使用寿命较长的优点[4]。

鉴于非接触式 IC 卡的飞速发展，国际标准化组织已开始对非接触式 IC 卡制定相应的标准。由于非接触式 IC 卡主要是在数据的传输方式上和接触式 IC 卡有所区别，所以其他的 IC 卡技术，如数据的存储、组织结构，数据的安全性等和接触式 IC 卡是一致的，故非接触式 IC 卡的标准只在射频传输界面和协议上作了相关的规定。在介绍非接触式 IC 卡的国际标准之前，先介绍一下有关的技术。

4.1　编码和调制

对射频识别系统来说，阅读器与 IC 卡之间的数据传输需要三个主要的功能块。按从阅读器到 IC 卡的数据传输方向，它们是阅读器中的信号编码（信号处理）和调制器（载波电路），传输介质（通路），以及应答器（IC 卡）中的解调器（载波回路）和信号译码（信号处理）。

信号编码系统的作用是使要传输的信息和它的信号表示尽可能最佳地与传输通道的性能相匹配。这里的处理包括有对信息提供某种程序的保护，以防止信息受干扰或相碰撞，以及对某些信号特性的蓄意改变。也称作在基带中的编码。

调制是改变高频载波的信号处理，即使其振幅，频率或相位，与调制的基带信号相关。

4.1.1 基带中的编码

可以用不同形式的代码来表示二进制的 1 和 0。射频识别系统通常使用下列编码法中的一种方法：

NRZ（反向不归零制）编码、曼彻斯特（Manchester）编码、单极归零制编码（Unipolar RZ）、差动双相编码（DBP）、米勒（Miller）编码、

差动编码和脉冲—间歇（PP）编码。

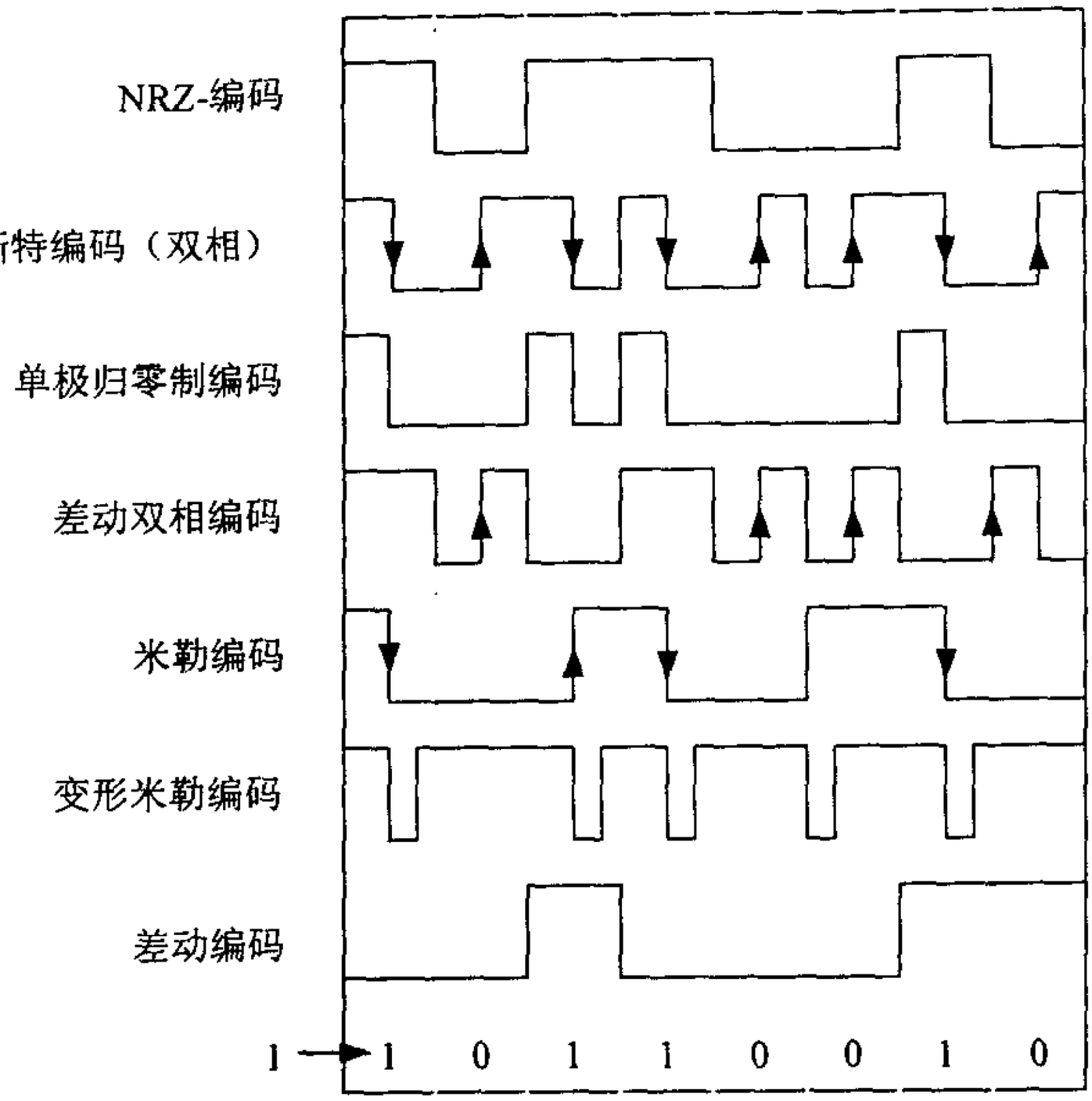


图4.1 RFID系统中常常改变形式代码来对信号编码

• NRZ 编码：“高”信号表示二进制 1，“低”信号表示二进制 0。在 FSK 或 PSK 调制中几乎仅仅使用 NRZ 编码。

• 曼彻斯特（Manchester）编码：在半个比特周期时的负边沿表示二进制 1，半个比特周期中的正边沿表示二进制 0。因此，曼彻斯特编码也称作分相编码（Split—Phase coding）。

曼彻斯特编码在采用副载波的负载调制时经常用于从应答器到阅读器的数据传输。

• 单极归零制编码：在第一个半比特周期中的“高”信号表示二进制 1，而持续整个比特周期的低信号表示二进制 0。

• 米勒（Miller）编码：在半比特周期内的任意边沿表示二进制 1，而经过下一个比特周期中不变的 1 电平表示二进制 0。一连串的零在比特

周期开始时产生电平交变，因此，对接收器来说，位节拍比较容易重建（如果需要的话）。

在为射频识别系统选择一种合适的信号编码系统时，应当注意不同的边缘条件。最重要的是调制后的信号频谱[33]，[40]以及对传输故障的敏感度。此外，对无源应答器（应答器的能量取自阅读器的 HF 场）来说，不允许由于信号编码与调制方法的不适当的组合而中断能量供应。

4.1.2 数字调制法

能量从天线以电磁波的形式发射到周围的空间。小心的改变电磁波的三种信号参数—功率、频率和相位之一，信息可以被编码，并传送到空间内的任一点去。信息（数据）对电磁波的影响过程称作调制，未调制的电磁波被称作载波。

传统的无线电技术中，主要是众所周知的模拟调制方法。根据电磁波的三个参数，可区分为振幅调制，频率调制和相位调制。所有其他的调制方法都是从这三种类型之一中引伸出来的。射频识别系统采用的调制方法是振幅键控（ASK）、频移键控（FSK）和相移键控（PSK）的数字调制法。

对每一种调制方法来说，都形成与载波对称的调制产物，即所谓的边带。边带的频谱和振幅都受基带中的编码信号的频谱以及调制方法的影响。边带可区分为上边带和下边带。

1．振幅键控（ASK）

在振幅键控时，载波振荡的振幅按二进制编码信号在两种状态 u_0 和 u_1 之间切换（键控）。$\hat{u}_1$ 可以取 $\hat{u}_0$ 和 0 之间的值。$\hat{u}_1$ 和 $\hat{u}_0$ 二者之比被称作键控度 m。

为了得到键控度，我们计算载波信号的键控的和非键控的振幅之间的算术平均值。

$$\hat{u}_m = \frac{\hat{u}_0 + \hat{u}_1}{2} \qquad [4.1]$$

从振幅变化 $\hat{u}_0 - \hat{u}_m$ 与平均值 $\hat{u}_m$ 之比可算出键控度。

$$m = \frac{\Delta \hat{u}_m}{\hat{u}_m} = \frac{\hat{u}_0 - \hat{u}_m}{\hat{u}_m} = \frac{\hat{u}_0 - \hat{u}_1}{\hat{u}_0 + \hat{u}_1} \qquad [4.2]$$

在 100%的振幅键控（ASK）时，载波振荡振幅在载波振幅之值 $2\hat{u}_m$ 和 0 之间进行切换（通—断键控）。在模拟信号（正弦形振荡）振幅调制时，

这将与 m=1（或 100%）的调制度相应[40]。

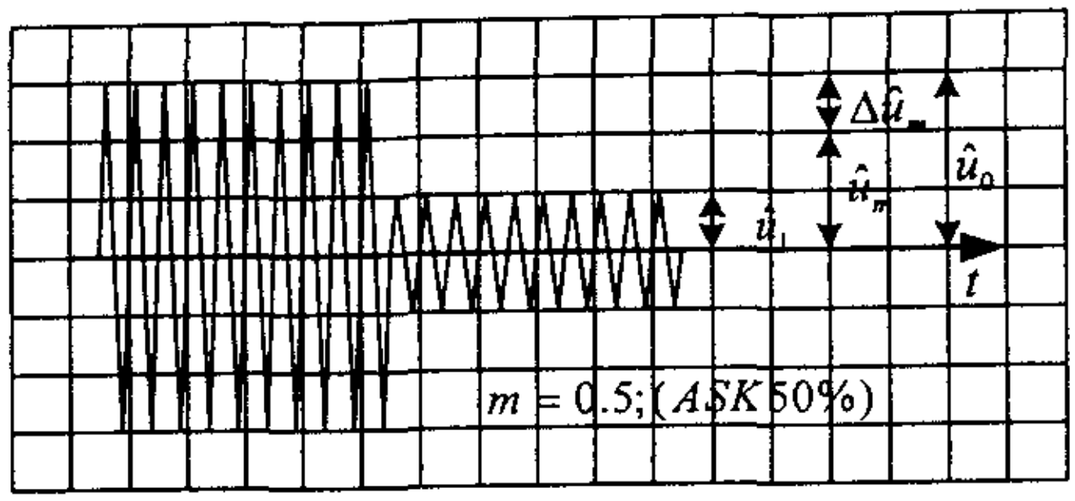


图4.2 ASK调制时，载波的振幅按二进制
编码信号在两种状态之间切换

上述计算键控度的方法与用模拟信号（正弦形振荡）的振幅调制时的调制度的计算方法相同。然而，在键控与模拟调制之间存在着一种重要的区别。在键控时，载波信号在未调制时的振幅为 $\hat{u}$。而在模拟调制时，载波在未调制时的振幅为 $\hat{u}_m$。

在一些文献中，有时把键控度当作键控过程中载波减小的百分比 m'：

$$m' = 1 - \frac{\hat{u}_1}{\hat{u}_0} \qquad [4.3]$$

对键控度<15%和键控度>85%来说，两种计算方法之间的区别可忽略不计。

二进制编码信号由 1 和 0 状态的序列组成，周期为 T 而比特持续时间为 τ。从数学角度来看振幅键控（ASK）调制，是编码信号 $u_{\text{code}}(t)$乘以载波振荡 $u_{\text{cr}}(t)$。对键控度 m<1 来说，可采用一附加常数（1 - m），使得非键控状态时仍可以用 1 乘 $u_{\text{HF}}(t)$。

$$u_{ASK}(t) = [m \cdot u_{code}(t) + 1 - m] \cdot u_{HF}(t) \qquad [4.4]$$

因此，通过编码信号频谱与载波频率 f_{cr} 的卷积或通过编码信号的傅里叶展开]乘以载波振荡，即可得到振幅键控（ASK）信号的频谱。他在上边带和下边带中包含了编码信号的频谱，与载波对称[40]。

2．2-FSK（频移键控）

2-FSK 是使载波振荡频率用二进制编码信号在两种频率 f_1 和 f_2 之间进行切换。

把两种特有的频率 f_1 和 f_2 的算术平均值定义为载波频率 f_{CR}。载波频率与特有频率之间的差被称作频差。

$$f_{CR} = \frac{f_1 + f_2}{2} \qquad [4.5]$$

$$\Delta f_{CR} = \frac{|f_1 - f_2|}{2} \qquad [4.6]$$

从时间函数的观点看来，可以把 2-FSK 信号看作是 f_1 和 f_2 的两种振幅键控信号的组合。因此，2-FSK 信号的频谱可由两种振幅键控振荡的频谱叠加得出。在射频识别系统中的基带编码，产生了非对称的频移键控：

$$\tau \neq \frac{T}{2} \qquad [4.7]$$

在这种情况下相对于中心频率的频谱Δf_{CR}也是不对称分布的。

3．2-PSK（相移键控）

相移键控，是将编码信号的二进制状态“0”和“1”转变成载波振荡相对基准相位的相应相位状态。对 2-PSK（相移键控）来说，是在相位状态 0° 和 180° 之间切换。

从数学的角度来看，在 0° 和 180° 之间的相互切换与载波振荡被“1”和“-1”相乘是一样的。

对键控比 τ / T 为 50%的情况来说，可以用下面的公式来计算 2-PSK（相移键控）的功率频谱[41]：

$$P(f) = [\frac{P \cdot T_S}{2}] \cdot [\sin c^2 \pi (f - f_0) T_S + \sin c^2 \pi (f + f_0) T_S] \qquad [4.8]$$

式中：P=发送功率；T_S=比特持续时间=τ；f_0=中心频率；

$\sin c(x) = \frac{\sin(x)}{x}$。

两个边带的包络线按照函数$(\sin(x)/x)^2$围绕着载波频率 f_0。这使得频率在 $f_0 \pm 1/T_S$、$f_0 \pm 2/T_S$、$f_0 \pm n/T_S$ 时为零。在频率范围 $f_0 \pm 1/T_S$ 内，90%的发送器功率被传输出去。

4．使用副载波的调制法

在无线电技术中，广泛地应用着一个调制的副载波：例如在 VHF 无线电广播中，频率为 38kHz 的立体声副载波随同基带声音通道一起传输。基带只包含单声道信号。为获得两个声音通道“*L*”和“*R*”所需的差分信号“*L-R*”可调制立体声副载波以“无声地”地传输。副载波的使用呈现为多电平调制。

就射频识别系统而言，用副载波的调制法主要用在频率范围为6.78MHz、13.56MHz 获 27.125MHz 的电感耦合系统中，而且是从应答器到阅读器的数据传输。电感耦合的射频识别系统的负载调制有着与阅读器天线上的高频电压的振幅键控（ASK）调制相似的效果。代替在基带编码的信号节拍中对负载电阻的切换，用基带编码的数据信号首先调制低频率的副载波。可以选择振幅键控（ASK）、频移键控（FSK）或相移键控（PSK）调制作为对副载波调制的方法。副载波频率本身通常是通过对操作频率的二进制分频产生的。对 13.56MHz 的系统来说，大多使用的副载波频率为847kHz（13.56MHz/16）、424kHz（13.56MHz/32）或 212kHz（13.56MHz/64）。已调的副载波信号则用于切换电阻。

在观察产生的频谱时，才能理解使用副载波带来的极大好处。

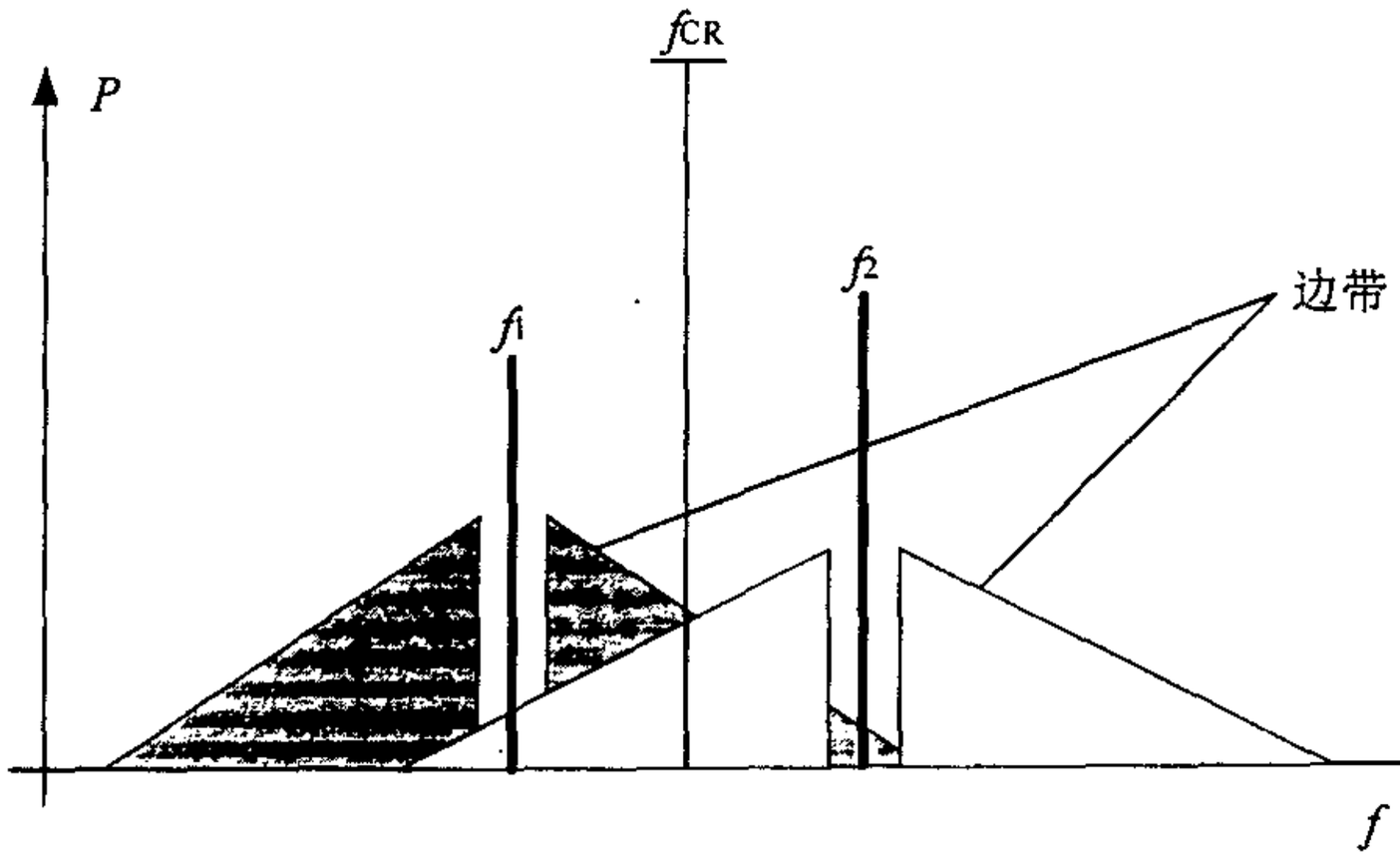


图4.3 用副载波的负载调制时的调制结果

副载波进行负载调制时，首先在围绕操作频率±副载波频率 f_H 的距离上产生两条谱线。真实的信息随着基带编码的数据流对副载波的调制被传输到两条副载波谱线的边带中。另一方面，如果采用的是在基带中进行的负载调制时，数据流的边带将直接围绕着工作频率的载波信号。

对很松散耦合的应答器系统来说，在阅读器的载波信号与接收的负载调制的调制边带之间的差别在 80~90dB 的范围内波动。通过数据流的调制边带的频移，可以将两个负载调制产物中之一滤出并解调。至于是使用 f_T+f_H 还是 f_T-f_H 都是无所谓的，因为在所有的边带中都包含了信息。

4.2 多路存取法—反碰撞法

在射频 IC 卡系统工作时，不能排除可能会有一个以上的 IC 卡同时处于阅读器的作用范围内。在这样的系统中存在着两种不同的基本通信形式：

第一种通信形式：从阅读器到 IC 卡的数据传输为第一种通信形式。发送的数据流同时被所有的 IC 卡接收。这可以同数百个无线电广播接收机同时接收一个发送信息相类比，而信息是由一个无线电广播发射机发射的。

第二种通信形式：在阅读器的作用范围有多个应答器的数据同时传输给阅读器。这种通信形式称作多路存取。

每个通信通路拥有规定的通路容量。这种通路容量是由这个通信通路的最大数据率以及供它使用的时间片确定的。分配给每个用户（IC 卡）的通路容量必须满足：当多个 IC 卡同时把数据传输给一个单独的阅读器时不能出现互相干扰（碰撞）。

对电感耦合的射频识别系统来说，只有阅读器中的接收部分作为共同的通路供阅读器作用范围内的所有应答器将数据传输给阅读器使用。最大数据率是由应答器天线的有效带宽和阅读器得出的。

射频识别系统多路存取技术的实现对应答器和阅读器提出了一些要求，因为必须使人们感觉不到浪费时间，必须可靠地防止由于应答器的数据（包）在阅读器的接收器中互相碰撞从而不能读出。在射频识别系统中的这种技术方法被称作反碰撞法。

4.2.1 多路存取方法

1．空分多路（SDMA）法

可以把空分多路法理解为在分离的空间范围内重新使用确定的资源（通路容量）的技术[42]。

一种可能性在于使单个阅读器的作用距离明显地减少，而把大量的阅读器和天线的覆盖面积并排地安置在一个阵列之中。因此阅读器的通路容量在相邻的区域内可重新使用。这样，当应答器经过这个阵列时就经过了整个配置中的某个天线的作用范围。因此，许多应答器——由于空间分布——可以同时读出。

另一种可能性在于：在阅读器上利用电子控制定向天线，该天线的方

向图直接对准某个应答器。所以，不同的应答器可根据在其阅读器作用范围内的角度位置互相区别开来。RFID 用的自适应 SDMA 由于天线的结构尺寸，只有当频率大于 850MHz（典型地是 2.45GHz）时才能使用。

2. 频分多路（FDMA）法

频分多路法是把若干个使用不同载波频率的传输通路同时供通信用户使用的技术。

负载调制的射频识别系统或反向散射系统使用频分多路的一种可能性在于：为了从应答器向阅读器传输数据，可使用不同的、独立的副载波频率。

3. 时分多路（TDMA）法

时分多路法是把整个可供使用的通路容量按时间分配给多个用户的技术。TDMA 首先在数字移动无线电系统的范围内推广使用。对射频识别系统来说，TDMA 构成了反碰撞法的具有最大量的一族。这种方法又可分为应答器控制（应答器驱动）和阅读器控制（询问驱动）法。

应答器控制法的工作是非同步的，因为这里对阅读器的数据传输没有控制。例如 ALOHA 法。按照应答器成功地完成数据传输后是否通过阅读器的信号而断开，又可区分为“开关断开”法和“非开关”法。

应答器控制法自然是很慢而又不灵活的。因此，大多数应用采取由阅读器作为主控制器的控制方法。通过一种规定的算法，在阅读器的作用范围内首先选择较大的应答器组中的一个应答器。然后在选择的应答器和阅读器之间进行通信。为了选择另外一个应答器，应该解除原来的通信关系，因为在同一时间内总是只建立起一个通信关系。并且，可以快速地按时间顺序操作应答器。因此，用阅读器控制的方法也称作定时双工传输法。

最灵活的和最广泛推广使用的方法是“二进制搜索算法”。对这种方法来说，为了从一组应答器中选择其中之一，阅读器发出一个请求命令有意识地将应答器序列号传输时的数据碰撞引导到阅读器上，在二进制搜索算法的实现中起决定作用的是：阅读器所使用的合适的信号编码必须能够确定碰撞的准确的比特位置。

4.2.2 常用的反碰撞法

1. ALOHA 法

所有多路存取方法中的最简单的方法就是 ALOHA 法。只要有一个数据包提供使用，这个数据包就立即从应答器发送到阅读器去。因此，这种

处理本身与应答器控制的、随机的 TDMA 法有关。

应答器是在一个周期性的循环中将数据发送给阅读器的。数据传输时间只是重复时间的一小部分，以致在传输之间长生相当长的间歇。此外，各个应答器的重复时间之间的差别是微不足道的。所以存在着一定的概率，两个应答器可以在不同的时间段上设置他们的数据，使数据包不互相碰撞。

在 ALOHA 系统中交换的数据包量 g 与在确定的时刻 t_0 同时发送的应答器数量（即 0、1、2、3…）相符。平均交换的数据包量 G 与经过一段观察时间 T 的平均值相符。平均交换的数据包量 G 可以用最简单的方法从一个数据包的传输持续时间τ计算出来：

$$G = \sum_{1}^{n} \frac{\tau_n}{T} \cdot r_n \qquad [4.9]$$

式中：n=1、2、3、...是系统中的应答器的数量，r_n=0、1、2、...是在观察时间 T 内由应答器 n 发送的数据包的数量。

吞吐率 S 等于 1，即是在传输期间无错误的传输数据包，在所有其他的情况下等于 0，因为或者没有发送，或者由于碰撞不能无错误的读出传输的数据。传输通路的（平均）吞吐率 S，可由交换的数据包量 G 得出：

$$S = G \cdot e^{(-2G)} \qquad [4.10]$$

如果观察交换的数据包量 G 和吞吐率 S 的关系，可以发现对较小的交换的数据包量来说，传输通路的大部分时间没有被利用；扩大交换的数据包量时，应答器之间的碰撞立即明显增加，80%以上的通路容量没有利用。成功概率 q，既无碰撞传输数据包的概率，可以从平均的交换的数据包量 G 和吞吐率 S 计算出来[42]：

$$q = \frac{S}{G} = e^{(-2G)} \qquad [4.11]$$

从数据包和平均交换的数据包量 G 的传输时间τ可以求出在观察时间 T 内的无错误传输的数据包的数量 k 和概率 $p(k)$，概率 $p(k)$是使用平均值 G/τ 的 Poisson 分布：

$$p(k) = \frac{[G\frac{T}{\tau}]^k}{k!} \cdot e^{[-G\frac{T}{\tau}]} \qquad [4.12]$$

2．时隙 ALOHA 法

使 ALOHA 法对比较小的吞吐率最佳化的途径就是时隙 ALOHA 法。应答器只在规定的同步时隙内才传输数据包。在这种情况下，对所有应答器所必需的同步应由阅读器控制。因此，这涉及到一种随机的、阅读器控制的 TDMA 反碰撞法。

与简单的 ALOHA 法相比，可能出现碰撞的时间只有一半那么多。

3．二进制搜索算法

实现“二进制搜索”算法系统的必要前提是能辨认出在阅读器中数据碰撞的比特的准确位置。为此，必须有合适的位编码法。首先要对 NRZ 编码和 Manchester 编码的碰撞状况作一比较。选择 ASK 调制副载波的负载电感耦合系统作为应答器系统。基带编码中的“1”电平使副载波接通，“0”使副载波断开。

• NRZ-编码：某位之值是在一个位窗（bit Window-t_{BIT}）内由传输通路的静态电平表示的。这种逻辑“1”编码为静态“高”电平，逻辑“0”编码为静态“低”电平。

如果两个应答器之一发送了副载波信号，那么这个信号由阅读器译码为“高”电平，且被认定为逻辑“1”。阅读器不能确定，读入的某位究竟是若干个应答器发送的数据相互重叠的结果或者是某个应答器单独发送的信号，信息校验和（奇偶校验、CRC 校验）的应用仅仅能够确定数据块中“任何一位”出现了传输错误。

• Manchester 编码：某位之值是在一个位（t_{BIT}）窗内由电平的改变（上升/下降沿）来表示的。这里，逻辑“0”编码为上升沿，逻辑“1”编码为下降沿。在数据传输过程中“没有变化”的状态是不允许的，并且作为错误被识别。

由两个（或多个）应答器同时发送的数位有不同之值，则接收的上升边和下降边互相抵消，以致在整个位窗的持续时间内接收器接收到的是不间断的副载波信号。在 Manchester 编码中对这种状态未作规定。因此，这种状态导致了一种错误，从而用这种方法可以按位回溯跟踪碰撞的出现。

为了实现“二进制搜索”算法系统，就要选用 Manchester 编码。

“二进制搜索”算法系统是由在一个阅读器和多个应答器之间规定的相互作用（命令和应答）顺序（规则）构成的。目前在于从较大的一组中选出任一个应答器。

为了实际实现这个算法系统，需要一组命令。这组命令能由应答器处理。此外，每个应答器拥有一个唯一的序列号。

• REQUEST(SNR) —请求（序列号）：此命令发送一序列号作为参数给应答器。应答器把自己的序列号与接收的序列号比较，如是小于或相等，则此应答器回送其序列号给阅读器。这样可以缩小预选的应答器的范围。

• SELECT（SNR）— 选择（序列号）：用某个（事先确定的）序列号作为参数发送给应答器。具有相同序列号的应答器将以此作为执行其他命令（例如读出和写入数据）的切入开关，即选择这个应答器。具有其他序列号的应答器只对 REQUEST 命令应答。

• READ-DATA — 读出数据：选中的应答器将存储的数据发送给阅读器（在实际的系统中，还有鉴别或写入、出纳登帐、取消预订等命令...）。

• UNSELECT — 去选择：取消一个事先选中的应答器，应答器进入“无声”状态，在这种状态中应答器完全是非激活的，对收到的 REQUEST 命令不做应答。为了重新活化应答器，必须暂时离开阅读器的作用范围（等于没有供应电压）以实现复位。

为了从较大量的应答器中发现一个单独的应答器，需要重复操作。其平均次数 L 取决于阅读器作用范围内的应答器总数 N，并且很容易求出：

$$L(N) = \lg(N) + 1 = \frac{\log(N)}{\log(2)} + 1 \qquad [4.13]$$

如果只有唯一的一个应答器处在阅读起作用范围内，那么只需要唯一的一次重复操作，以便发现应答器的序列号—在这种情况下不出现碰撞。如果有一个以上的应答器出现在阅读器作用范围内，那么重复操作的平均数很快增加。

4．动态的二进制搜索法

上述二进制搜索法，不仅搜索的范围标准，而且应答器的序列号总是一次次完整地传输的。然而，在实际中应答器的序列号按系统的规模可能长达 10 个字节，以致不得不传输大量的数据，而仅仅是选择一个单独的应答器。如果我们更仔细地研究阅读器和单个应答器之间的数据流（见图 4.4），就可以得出：

• 命令中（X-1）~0 各位不包含给应答器的补充信息，因为（X-1）~0 各位总是被置为“1”的。

• 应答器应答的序列号的 N~X 各位不包含给阅读器的补充信息，因为 N~X 这些位是已知且给定的。

由此可见：传输的序列号的各自的互补部分是多余的，本来也是不必传输的。

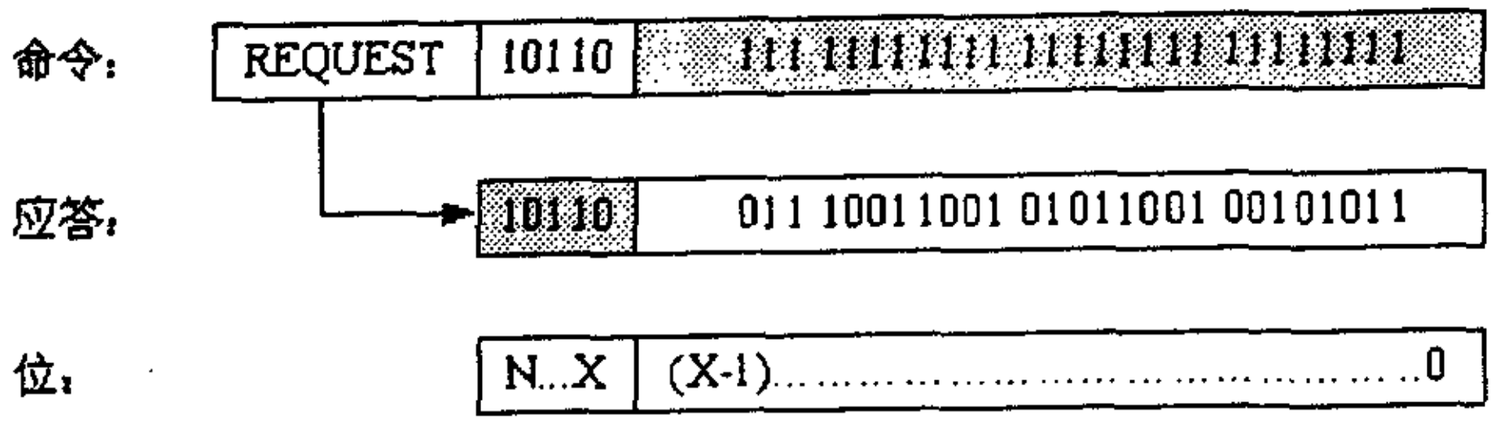


图4.4 在搜索一个4字节序列号时，阅读器的命令（第n次重复操作）的应答。由于命令和应答中传输的数据大部分是多余的（如图中灰色部分所表示的那样）。用X表示最高位的位置，在此最高位上出现了位碰撞

这样可以得出一种最佳的算法：代替序列号的两个方向上完整地传输，序列号或搜索的范围标准的传输现在简单地改变为部分位（X）。

阅读器在 REQUEST（请求）命令中只发送要搜索的序列号的已知的部分作为搜索的依据，然后中断传输。所有在（N~X）位中的序列号与搜索依据相符的应答器，则传输它们的序列号的剩余各位即（X-1）位为应答。在 REQUEST 命令中的附加参数（有效位的编号）将下余各位的数量通知应答器。

4.3　非接触式（射频）IC 卡的国际标准

非接触式 IC 卡以作用距离的不同而分为三个不同的标准。密耦合 IC 卡标准 ISO/IEC 10536 主要是在 1992 年到 1995 年间发展的。近耦合和疏耦合 IC 卡标准的制定工作—国际标准 ISO/IEC 14443 和 ISO/IEC 15693—大约是 1995 年开始着手进行的，两项标准在 2000 年后才正式有效完成。

近耦合 IC 卡的作用距离在 10cm 左右，目前绝大部分的民用系统都采用的是近耦合 IC 卡。所以，以下将主要就近耦合 IC 卡系统作介绍。

ISO/IEC 14443 标准分为四个部分。其中第一部分规定了 IC 卡的机械性能—物理特性。规定非接触式 IC 卡的尺寸应与国际标准 ISO/IEC 7810 中的规定相符，即 85.72mm×54.03mm×0.76mm±容差[38]。

标准的第二部分规定了射频能量和信号接口，第三部分则规定了卡的初始化和反碰撞，最后一部分则规定了卡的选择应答和传输协议。下面将对其进行详细介绍：

4.3.1 ISO/IEC 14443-2：射频信号接口—编码和调制方法

1．能量传送

耦合 IC 卡的能量是通过发送频率为 13.56MHz 的阅读器的交变磁场来提供的。IC 卡中包含有一个大面积的天线线圈。典型的线圈具有 3~6 匝导线。

由阅读器产生的磁场不允许超过或低于极限值，即 $1.5A/m \le H \le 7.5A/m$。$H_{min} \le 1.5A/m$ 用为近耦合 IC 卡的动作场强 H_{min} 时，只有在下述情况才能有保证：通过产生的场强恰好为 $1.5A/m$ 的阅读器在与发送天线的距离 x=0 时能够读出具有动作场强为 $H_{min} = 1.5A/m$ 的 IC 卡[38]。

如果阅读器的场强以及近耦合 IC 卡的动作场强是已知的，那么可以估计系统的作用距离。根据国际标准 ISO14443 中的典型的阅读器的场强曲线，IC 卡的动作场强为 $1.5A/m$，在这种情况下得出的作用距离为 10cm。

2．信号接口

国际标准 ISO14443 在阅读器和近耦合 IC 卡之间的数据传输规定了两种完全不同的方法：A 型和 B 型，一张 IC 卡只需两种通信方法之一来支持。然而，一个符合标准的阅读器必须能够以任意方法通信，以便支持所有的 IC 卡。这要求阅读器在“闲置”状态时能在两种通信方法之间周期的转换[1]。

（1）通信界面—A 型

对 A 型 IC 卡来说，使用改进的 Miller 编码的 100%振幅键控调制作为从阅读器到 IC 卡传输数据的调制方法[15]。为了保证对 IC 卡的不间断的能量供应，回扫间隙的长度大约只有 2~3μs。标准中详细地规定了，由阅读器产生的高频信号进入对起振和停振状态时回扫间隙的要求。

为了从 IC 卡到阅读器传输数据，使用副载波的负载调制方法。副载波频率为 f_H=847kHz（13.56MHz/16）。副载波的调制是通过对曼彻斯特编码的数据流的副载波的键控来完成的[38]。

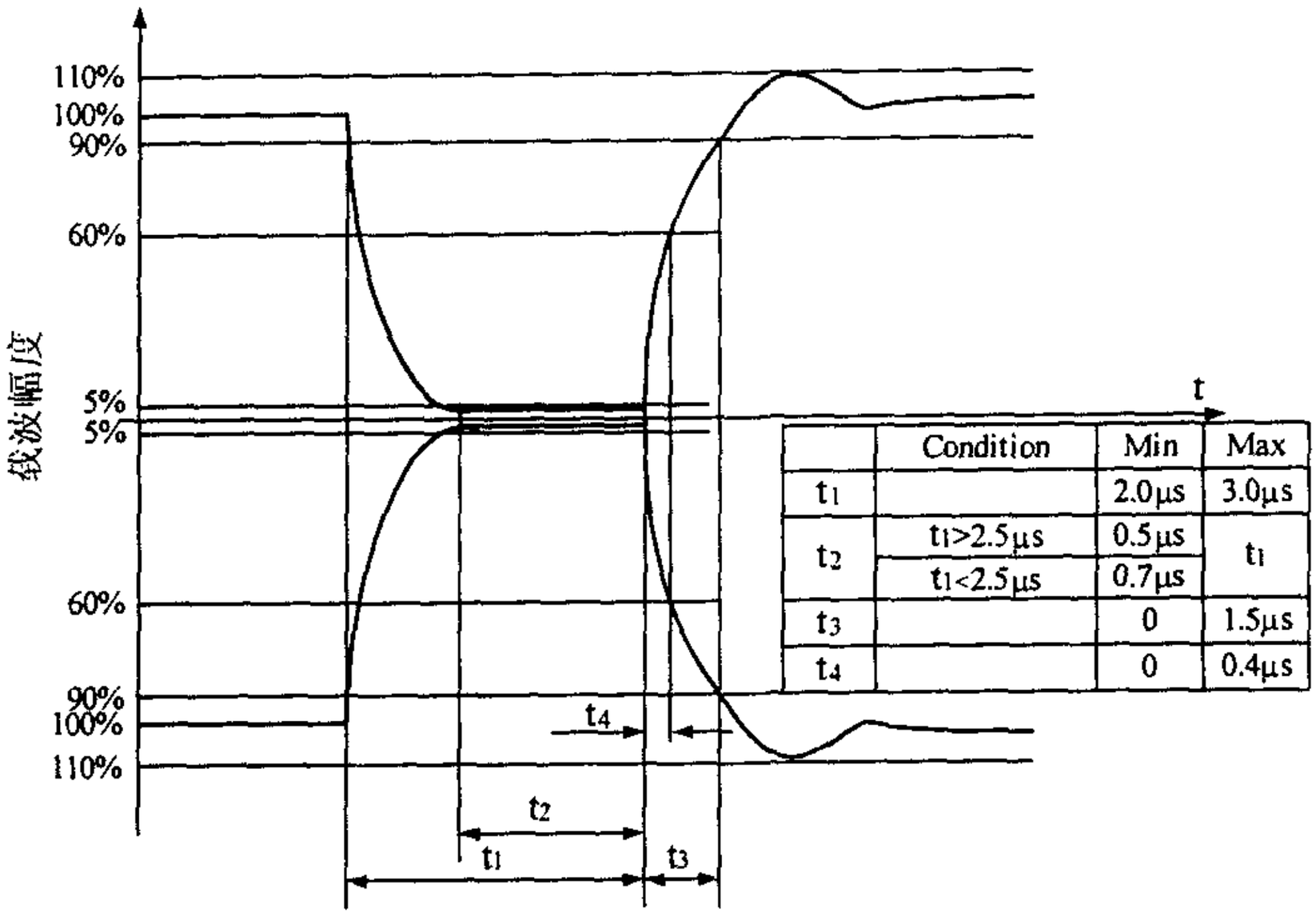
在两个传输方向上，波特率为 f_{Bd}=106kbit/s（13.56MHz/128）。

（2）通信界面—B 型

对B型IC卡来说，使用10%的ASK调制作为从阅读器到IC卡的数据传输的调制方法。使用简单的NRZ编码。标准中详细地规定了高频信号在起振和停振状态时进入0/1的过渡状态，由此可以计算出对发送天线的质量要求。

为了从IC卡向阅读器传输数据，B型也使用了有副载波的负载调制。副载波频率为f_H=847kHz（13.56MHz/16）。副载波的调制是通过对NRZ编码的数据流的副载波的180°相移键控（BPSK）来完成的。

在两个传输方向上，波特率为f_{Bd}=106kbit/s（13.56MHz/128）。



	Condition	Min	Max
t_1		2.0μs	3.0μs
t_2	t_1>2.5μs	0.5μs	t_1
	t_1<2.5μs	0.7μs	
t_3		0	1.5μs
t_4		0	0.4μs

图4.5 回扫间隙 [18]

4.3.2 ISO/IEC 14443-3：初始化和反碰撞

1．登记（polling）

如果一个近耦合的IC卡处于某阅读器的作用范围内，首先就要在阅读器和IC卡间建立起通信关系。为了检出进入到阅读器的能量场的近耦合IC卡，阅读器重复发出请求命令REQA/REQB并查询应答ATQA/ATQB，这一过程称为登记（polling）[38]。

REQA和REQB分别对采用A型和B型规范的IC卡所发出的请求信

号。

符号	说明	最大值
t_{ORA}	激活场和第一个 REQA 命令的起始位之间的登记复位时间	5000μs
t_{ORB}	激活场和第一个 REQB 命令的起始位之间的登记复位时间	5000μs
t_{ARA}	任一 A 型阅读器命令的最后一位与 REQA 之间的登记复位时间	500μs
t_{BRB}	任一 B 型阅读器命令的最后一位与 REQB 之间的登记复位时间	
t_{ARB}	任一 A 型阅读器命令的最后一位与 REQB 之间的登记复位时间	5000μs
t_{BRA}	任一 B 型阅读器命令的最后一位与 REQA 之间的登记复位时间	5000μs

表 4.1　近耦合 IC 卡的登记复位时间[38]

近耦合 IC 卡应该遵守的最大登记复位时间规定如表 4.1 所示。

2．初始化和防冲突

标准的这一部分首先规定了协议（帧）的结构。并规定了为选择一个单独的 IC 卡所使用的反碰撞方法。因为对 A 型和 B 型来说不同的调制方法是以不同的协议和反碰撞方法为前提的，所以在这项标准的第 3 部分将 A 型和 B 型两种类型分别规定。

（1）A 型卡

只要有一个 A 型 IC 卡到达了阅读器的作用范围内，并且有足够的供应电能可以使用，卡中的微处理器或 ASIC 就开始工作。在执行了一些预置程序（在复合卡的预置程序中还必须测试：IC 卡是在非接触的还是接触的工作模式中）后，IC 卡即处于所谓的闲置状态。此时，阅读器可以同作用范围内的另外的 IC 卡交换数据。然而，处于“闲置状态”的 IC 卡决不能对阅读器传输数据给另外的 IC 卡起反应，从而不干扰正在进行的通信。

如果 IC 卡在 IDLE 状态接收到了有效的 REQA 命令（请求 A），则回送对请求的应答字组 ATQA（ATR）给阅读器。为了保险，使发送给阅读起作用范围内的另外一个 IC 卡的数据不致错误地解释 REQA 命令，它仅由七个数据位组成。而回送的 ATQA 字组由两个字节组成，并且在标准帧中被回送。

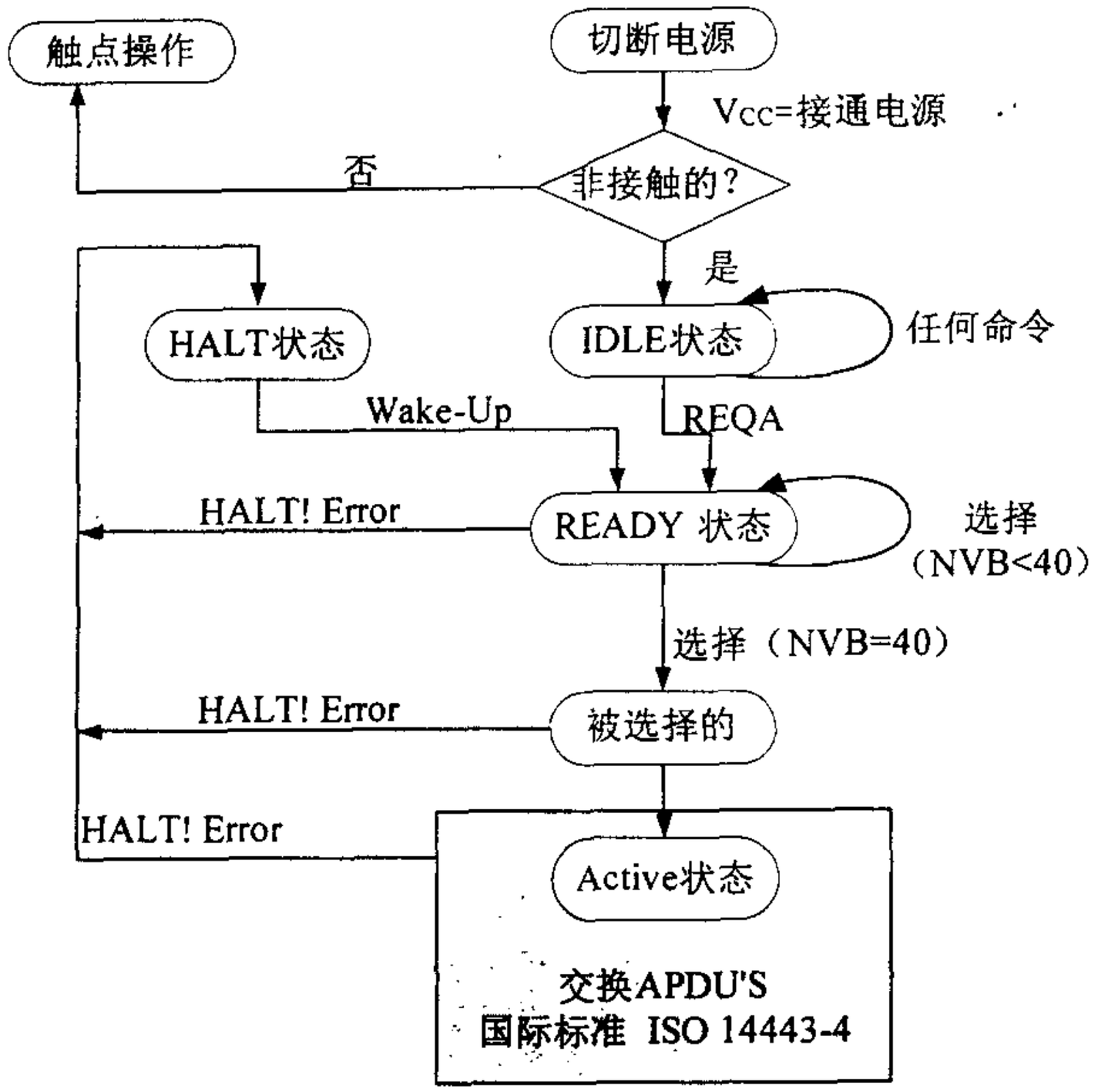
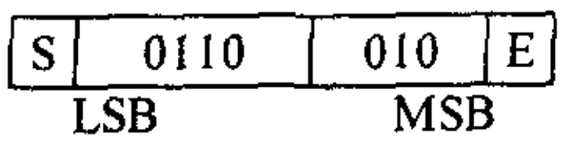


图4.6 根据国际标准 ISO 14443 的 A 型卡的状态图

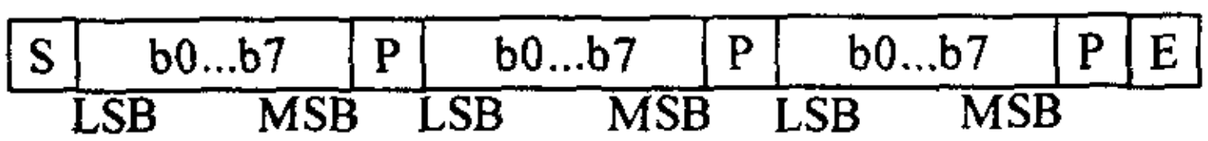
当 IC 卡对 REQA 命令 A 作了应答之后，IC 卡处于 READY 状态。阅读器现在识别出：在作用范围内至少有一张 IC 卡存在，并通过发送 SELECT 命令启动反碰撞算法。这里采用的反碰撞方法是动态的“二进制搜索树”算法。为了传输检索的准则和应答 IC 卡，采用了面向位的帧，这样，在发送一方发送任意数量的字节后都能在阅读器和 IC 卡之间转变成相反的传输方向。SELECT 命令的 NVB 参数是为了说明检索的准则的实际长度用的。

简单的序列号的长度为 4 字节。如果通过反碰撞算法去查找一个序列号，那么阅读器在 SELECT 命令中要发送完整的序列号（NVB=40h），以便选择合适的 IC 卡。具有所查找的序列号的 IC 卡用选择应答 SAK 来确认这条命令，并处于 ACTIVE 状态，即选择状态。而在这方面的一个特殊情况是：不是所有的 IC 卡的序列号都是 4 字节长（单长度）。标准也允

许有 7 字节长的序列号（倍长度），甚至允许 10 字节长度的序列号（三倍长）。如果选择的 IC 卡可供使用的序列号为倍长度或三倍长度的序列号，那么这是 IC 卡在给阅读器的 SAK 中通过设定一个“串联位”（b3=1）发出信号，并表明 IC 卡保持 READY 状态。这样。阅读器再次启动反碰撞算法，以便求出序列号的第二部分。对 10 字节长的序列号来说，必须重复使用反碰撞算法，甚至第三次使用反碰撞算法。现在为了使 IC 卡发出对应的信号，应该表明启动的算法查找的是序列号的哪一部分，这就要在 SELECT 命令中能区分为三个串联级（CL1、CL2 和 CL3）。在查找序列号时，必须总是首先从串联级 1 启动。为了排除较长的序列号的碎块与一个较短的序列号偶然地相同，在反碰撞算法中将所谓的串联标志（CT=88h）在预先规定的位置上插入 7 字节或 10 字节长的序列号中。因此，对较短的序列号来说，在相应的字节位置上此标志从未出现过。



A型IC卡的阅读器的REQUEST命令仅由七个数据位组成。
一定要排除把发送给另外一个IC卡的有用数据错误地解释为REQUEST命令（S=帧起始位，E=帧结束位）



除REQA命令外，在反碰撞过程中阅读器与 IC卡之间的所有数据都作为标准帧传输。总是以帧起始位（ S）开始，接着是任意数量的数据字节。每个数据字节用一个奇偶校验位以防止传输错误。用帧结束位（ E）结束数据传输

图4.7 A型卡的帧结构[38]

还应当关注阅读器的命令与IC 卡的应答之间的准确定时和IC 卡的同步状态，因此应答器的发送只能在固定时间间隙中的规定时刻完成。

最后接受的字节	要求的时间响应
“1”	$t_{RESPONSE} = (N \cdot 128 + 84) \cdot t_0$
“0”	$t_{RESPONSE} = (N \cdot 128 + 20) \cdot t_0$

N=9 适用于对 REQA、WakeUp 命令或 SELECT 命令的应答。对所有其他命令（例如应用命令）来说，必须是 $N \geq 9$（*N*=9、10、11、12、...）。

（2）B 型卡

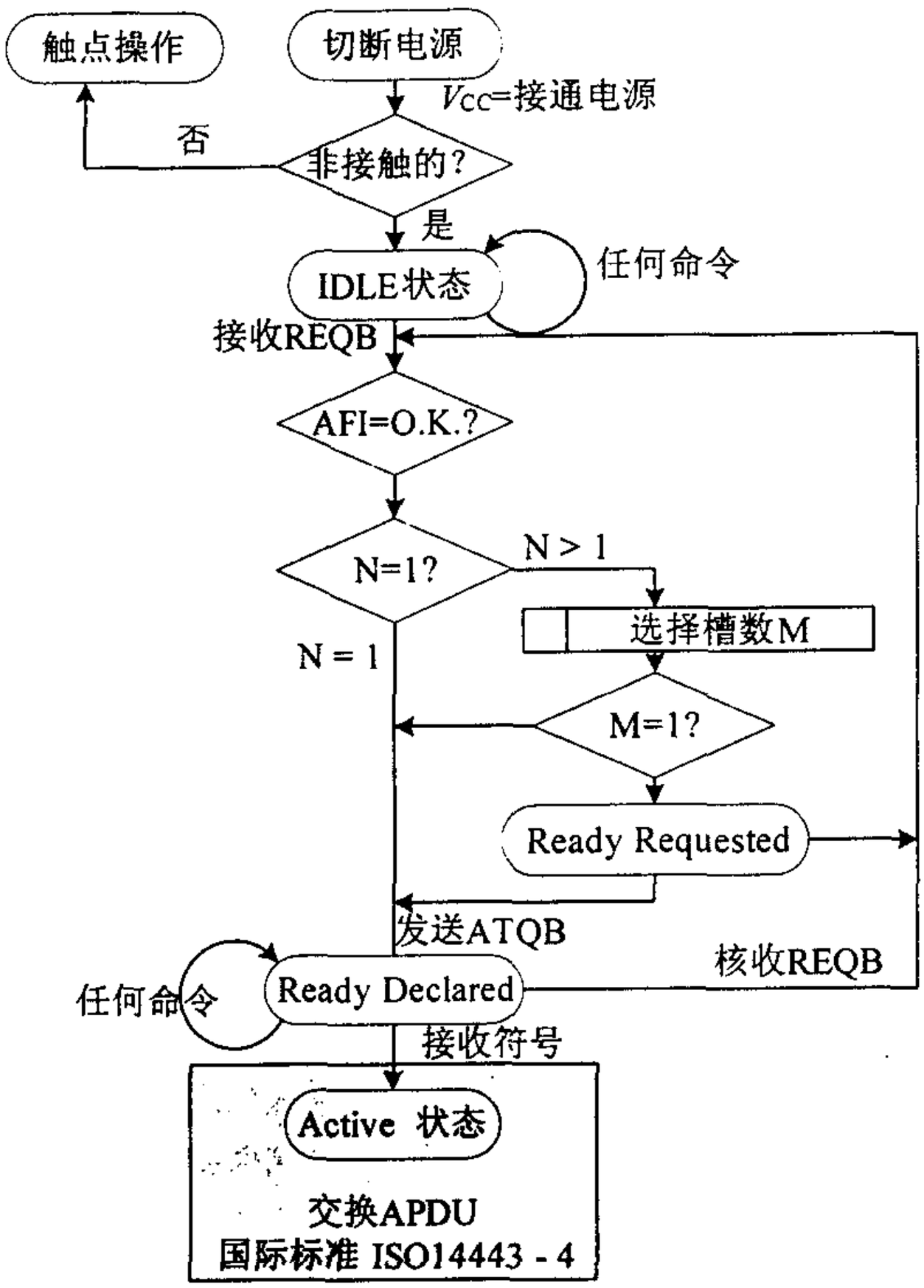


图4.8 根据国际标准ISO 14443的B型IC卡的状态图

如果一个 B 型 IC 卡被置入了阅读器的作用范围内，那么 IC 卡在执行一些预置程序后首先到达 IDLE 状态，并等待接收有效的 REQB（REQUESTB）命令。

对 B 型 IC 卡来说，通过发送 REQB 命令可以直接启动反碰撞算法。使用的方法是动态的 Slotted - ALOHA 法（动态时隙 ALOHA 法）。对这

种方法来说，阅读器的槽数可以动态的变化。可供使用的槽的数量编码在命令 B 的参数中。为了能够在选择 IC 卡时先行预选，REQB 命令具有另外一个参数，即“应用系列标识符”（AFI），用这个参数做检索准则可事先规定某些应用。

当 IC 卡接收到有效的 REQB 命令后，IC 卡就查明：在其存储的应用中是否有参数 AFI 中预选的应用组存在。若有，则用 REQB 命令的参数 M，以便求出供反碰撞使用的槽数。如果可供使用的槽数达于 1，那么必须在每个IC卡的随机数发生器中规定槽的号码号IC卡在读槽内将它的应答传输给阅读器。为了保证 IC 卡与槽同步，阅读器在每个槽开始时发送自己的槽标志。IC 卡现在等待着：直到事先规定的槽的槽标志被接收时（Ready – Requested 状态），即发送器对 REQB 命令的应答 ATQB（对 Request - B 的应答）。

Apf	AFI	PARAM	CRC
1字节	1字节	1字节	2字节

REQB命令的结构。反碰撞标志（Apf）具有（05h）的备用值。
该值在另外的命令的参数NAD中不准使用，以便保证排除混淆

Apa	PUPI（标识符）	应用数据	协议信息	CRC
1字节	4字节	4字节	2字节	2字节

ATQB结构。（对Request - B 的应答）

Apn	CRC
1字节	2字节

槽标志的结构，槽的流水号依次在参数 Apn中编码：
Apn=‘nnnn0101b’=‘n5h’；n=槽标志1~15

NAD	数据	CRC
1字节	N字节	2字节

在阅读器和B型IC卡之间的双向传输应用数据的标准帧的结构。
NAD（节点地址）的值X5h（05h、15h、25h、...E5h、F5h）应该保留给反碰撞命令，以便保证排除同应用命令的混淆

图4.9 B型IC卡的帧结构[38]

槽标志发送后，阅读器经过很短时间就可以确定：在当前的槽内是否

有一个 IC 卡已经开始传输对 REQB 的应答。如果不是这种情况，那么该槽可籍发送逐个的槽标志简单地中断，以便节省时间。

由 IC 卡发送的请求应答 ATQB 将一系列的有关 IC 卡的重要信息参数传输给阅读器。为了能够选择 IC 卡，请求应答 ATQB 首先包含有 4 字节的序列号。与 A 型 IC 卡相反，B 型 IC 卡的序列号不是必然的与芯片紧密相连，而是可以由一随机数组成。每次加电复位可以另行求出随机数（PUPI，拟惟一 PICC 标识符）。在参数“协议信息”内将非接触的界面参数编码、例如 IC 卡可能的最大波特率、最大帧参数或者有关选择的协议说明。此外，参数“应用数据”可以包含有关在 IC 卡上多种可供应用（多功能 IC 卡）的信息。

阅读器无错误的接收到 IC 卡的 ATQB，就可以有针对性地选择一个 IC 卡。这是用第一个应用命令来完成的。这个应用命令由阅读器发送。命令的结构与标准帧相符，而该帧的附加信息接在特殊的首标，即在位于前面扩大的 ATTEIB – Prefix 中。

图4.10 如果IC卡的标识符与首标的标识符（PICC）相符，那么通过用位于前面的ATTRIB - Prefix发应用命令可以选择一个IC卡

ATTRIB – Prefix 本身是由要选择的（事先求出的）卡序列号（PUPI）和一个参数字节组成的。参数字节包含有关于阅读器的可能的通信参数的重要信息，例如阅读器的命令和 IC 卡的应答之间的最大等待时间，或者负载调制器中的副载波信号的接通与由 IC 卡发送的第一个数据位之间的必要的等待时间。

4.3.3 ISO/IEC 14443-4：选择应答和传输协议

1．激活序列

（1）A 型 IC 卡

开始时，为了得到 ATS（Answer to Select），阅读器必须检查 SAK（Select Acknowledge）字节。SAK 的定义在第 3 部分中给出。假如 SAK 表示已根据 UID 选中了一张近耦合 IC 卡。阅读器将发送 RATS（Request for answer to select），以后 IC 卡发送 ATS 来回答 RATS。假如阅读器检查

到它不支持该IC卡或协议，它将置IC卡于HALT状态或使用PPS（Protocol and Parameter Selection）转到另一个支持的协议。

IC卡完成一次交易之后，将被置于HALT状态。

（2）B型IC卡

其描述在第3部分中，定义于阅读器可选的RATS、ATS和PPS请求、PPS应答中。

2．协议T=CL，半双工分组传输协议

协议所用的帧格式在第3部分中规定。协议的设计根据开放系统互联（OSI）参考模型的分层原则，定义了4层。

- 物理层交换字节遵循[14443-3]。
- 数据链路层交换分组定义
- 会话层结合数据链路层，以求得最小的开销。
- 应用层处理命令，在任一方向至少交换一个分组或分组链。

（1）分组格式

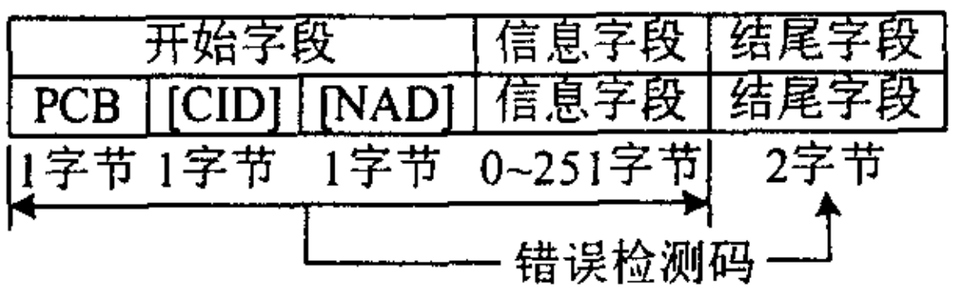


图4.11 分组格式

分组是帧的专有类型，是一个有效的T=CL数据格式。包括开始字段（必备）、信息字段（可选的）和结尾字段（必备）。

a) 开始字段

该字段是必备的，最多由3个字节构成。

① 协议控制字节PCB（Protocol control byte）（必备）。

② 卡标识符CID（Card Identifier）（可选）。

③ 节点地址字段NAD（Node Address）（可选）。

- PCB包含控制数据传输所需的信息，定义了三种基本分组类型：

① I－block（信息分组）：包含应用层所用的信息，另外，还包含了正的或负的确认。

② R－block（接受准备分组）：包含正的或负的确认，该确认与最后接受的分组有关。

③ S－block（管理分组）：用于在阅读器和 IC 卡之间交换控制信息、INF 字段是否存在有赖于他的控制。

· CID：用于访问指定的 IC 卡，该 IC 卡的标识符是在卡激活时被指定的。IC 卡激活时，CID 是固定不变的，当 IC 卡成功进入 HALT 状态时，CID 失效。

· NAD：在 IC 卡和阅读器之间建立逻辑连接。NAD 字节的编码：

b_8 和 b_4 都为 0，$b_7 \sim b_5$ 为 DAD（目标节点地址），$b_3 \sim b_1$ 为 DAD（源节点地址）。阅读器发送的第一个分组的 NAD 建立 SAD 和 DAD 的联系，用此方法定义了一个逻辑连接。如果 SAD 和 DAD 都为 0，表示节点地址无用，则 NAD 字段可以略去。SAD 和 DAD 相同的 NAD，作为 RFU。

如果 IC 卡支持 NAD 字段，则由阅读器来决定数据传输时是否用到 NAD。NAD 字段仅在 I－block 中有效，如果用到分组链，仅在链的第一个 I－block 饱含 NAD 字段。

b) 信息字段 INF（Information Field）

INF 字段是可选的。如有 INF，在 I－block 中，为应用数据；在 S－block 中，不是应用数据而是状态信息。

c) 结束字段

该字段包含发送分组的错误检测码 EDC（Error Detection Code）。

协议规定使用循环冗余校验码 CRC（Cycle Redundancy Check）。

（2）等待时间

a) 帧等待时间 FWT（Frame Waiting Time）：

FWT 用以检查传输错误或 IC 卡无应答。IC 卡用一个 S－block 请求来扩展的等待时间 WTX（Waiting Time Extension）。该请求有一字节信息字段，内含等待时间扩展倍增因子 WTXM（Waiting Time Extension Multiplier），用下列公式计算 FWT 的临时值。

$$FWT_t = FWT \cdot WTXM$$

当无分组链接时，临时 FWT 在 IC 卡发出下一个 I－block 后失效，否则提供给整个链中的所有 I－block。

b) 帧保护时间 FGT（Frame Guard Time）：

定义两分组之间的最小时间为 FGT，接受分组和发送分组之间的最小延迟为 FGT。

第五章　射频 IC 卡的发展—CPU 卡

射频 IC 卡由于采用的能量供给方式的限制，导致对内嵌芯片功耗的要求比较严格。而微处理器的功耗一直比较大，阻碍着 CPU 嵌入到射频 IC 卡中。而 CPU 卡在安全性和多应用方面体现出来的灵活和可靠的优势，使得 ASIC 射频 IC 卡在很多对安全性要求较高、以及使用环境变化比较敏感的区域的使用受到了限制。为了使射频 IC 卡的适用领域不断扩展和其本身的进一步发展，在射频 IC 卡中实现真正的智能卡芯片是当前射频 IC 卡发展的重点和趋势[11]。

5.1　CPU 卡技术

在前面的章节对 IC 卡的分类中已经对 CPU 卡做过一些简单的介绍。它是现代半导体技术及计算机技术最新发展的一个典型成果，在一个大约 0.3 立方毫米的半导体晶片上，不仅集成了功能复杂的微处理器，而且还配置了容量极大、类型不同的存储器和逻辑控制电路。这使得 CPU 卡具有更严密的数据安全性，更加广泛的应用灵活性和更加强大的功能扩展性。可以说，一个 CPU 卡片就是一台非常小的微型计算机系统。微机系统通常都由硬件和软件构成，下面就从硬件和软件两方面对 CPU 卡作一介绍。

5.1.1 CPU 卡的芯片技术

CPU 卡从电源的供给方面可以分为无源型和有源型两种。在无源型的 CPU 卡中，芯片电路中采用了一种混合存储器结构，其中一部分采用易失性存储器（如 RAM 部分）作为 CPU 的内存储器。而在有源型的 PCMCIA 卡中，则是采用高性能的微型电池来保持整个存储卡内的数据。它们都是采用的并行传输方式。

为了降低功耗，在 CPU 卡中使用的易失性存储器一般采用 CMOS 技术，并具有高速存取数据的能力。

在 CPU 卡中，整个数据存储区是一个没有逻辑分区的整体。其功能分区是由发行单位根据实际的应用需要，在初始的开发阶段将分区功能的

划分要求设计在监控程序之中，或者由驻留的卡片操作系统按文件的形式来定义。在卡片初始化之后，其内部各功能判定识别与操作完全交由监控程序或操作系统来解释和控制执行。

智能卡内的集成电路一般包括 CPU、ROM（或 EPEROM）、RAM、EEPROM 和安全逻辑等。现在一般智能卡内的 CPU 都是采用微控制器 MCU（Micro Controller Unit）核心，而不必重新设计。

和微处理器一样，在 CPU 卡芯片中设计了多个特殊功能寄存器（SFR），如串口寄存器 （Serial Port Registers）、中断寄存器（Interrupt Registers）、存储器控制寄存器（Memory Control Register）和随机字控制寄存器（Random Word Control Register）等。它们的主要作用是用于记录芯片运行状态的各种标志。在其中不是所有的地址都被占用，而未占用的地址可能不包含在芯片中。用户的软件一般不应写在这些未被列出的地址，因为他们有可能用于未来产品所需求的新的功能上。

CPU 卡芯片中存储器结构主要由三部分组成：随机存取数据存储器（RAM）；可擦除可编程数据/程序只读存储器（EEPROM）和只读存储器（ROM）或闪速、可变程序存储器（FPEROM）。

一般在 CPU 卡芯片生产时，在 ROM 或 FPEROM 里装入了一段引导程序，使得用户可利用此引导程序来下装自己的“应用监控程序”。

芯片中的三种存储器都具有三种工作模式，即：测试模式、下装模式和功能模式。

一些 CPU 卡芯片中有可编程串行接口，可按 ISO7816 标准定义的方式执行字节传送。数据字节装在移位寄存器中。CPU 通过对串口控制寄存器写入不同值，来控制接口。接口当前的状态被记录在串口寄存器中。在每次传送处理之后，CPU 都会读取串口的状态。

为了进行认证，随机字发生器也是经常出现在 CPU 卡芯片中的部分。

安全保护功能电路在 CPU 卡芯片中很重要的部分，在芯片的设计中考虑多种保护芯片运行的功能。如传输代码保护：在芯片的 EEPROM 存储器里开辟了一个 32 位的一次性可编程的“传输代码”存储区。芯片在发货时，由生产厂家在芯片内写入一组“传输代码”。这组代码是唯一的且不可更改地保存在这一特殊功能存储区里。在芯片发行前的初始化处理时，首先需要输入“传输代码”并与之比较。只有在一致的情况下，才能对卡片继续进行处理。

5.1.2 CPU 卡的操作系统—COS

COS 的全称是 Chip Operating System（片内操作系统），它一般是紧紧围绕着它所服务的智能卡的特点而开发的。COS 是一个专用系统而不是通用系统，不同卡内的 COS 一般是不相同的。因为 COS 一般都是根据某种智能卡的特点及其应用范围而特定设计开发的，尽管它们完成的功能大部分都遵循着同一个国际标准。另外，COS 本质上接近于监控程序，而不是真正意义上的操作系统，这一点至少在目前看来仍是如此。在当前阶段，COS 所需要解决的主要还是对外部的命令如何进行处理、响应的问题[31]。

COS 一般都是紧密结合智能卡内存储器分区的情况，按照国际标准（ISO/IEC 7816 系列标准）中所规定的一些功能进行设计、开发的。但是，由于智能卡的发展速度很快，而标准的制定周期相对比较长一些，因而许多厂家又各自都对自己开发的 COS 作了一些扩充。

COS 的主要功能是控制智能卡和外界的信息交换，管理智能卡内的存储器并在卡内部完成各种命令的处理。其中，与外界进行信息交换是 COS 最基本的要求。COS 的功能可以概括如下：

- 芯片运输到用户（指发行商）时对传输代码的比较处理，以及发卡时的个人化处理。
- 一次交易后的完整处理：

① 插卡后的初始化处理以及向接口设备发回复位应答 ATR（Answer to Reset）。

② 数据自动恢复（防撕裂处理）。CPU 卡的处理过程比逻辑加密卡复杂，通常采用数据备份的方法来实现数据的自动恢复功能。

③ 接口设备和 IC 卡之间以命令 – 应答方式进行处理。

1．COS 的体系结构[5]

所有的 COS 都必须能够解决至少三个问题，即文件操作、鉴别与核实、安全机制。事实上，鉴别与核实和安全机制都属于智能卡的安全体系的范畴之中，所以，智能卡的 COS 中最重要的两方面就是文件与安全。而从阅读器发出命令到卡给出响应的完整过程则可以分成四个阶段，或者说是四个功能模块：传送管理器（TM）、安全管理器（SM）、应用管理器（AM）和文件管理器（FM）。其中，传送管理器用于检查信息是否被正确的传送。这一部分主要和智能卡所采用的通信协议有关。安全管理器则

用于对所传送的信息进行安全性的检查或处理，防止非法的窃听或侵入。应用管理器则用于判断所接受的命令执行的可能性；文件管理器通过核实命令的操作权限，最终完成对命令的处理。对于一个具体的COS命令而言，这四个阶段并不是一定都必须具备。

（1）传送管理（Tansmission Manager）

传送管理主要是依据智能卡所使用的信息传输协议，对由阅读器发出的命令进行接收。同时，把对命令的响应按照传输协议的格式发送出去。由此可见，这一部分主要和智能卡具体使用的通信协议有关；而且，所采用通信协议越复杂，这一部分实现起来也就越困难、越复杂。

传送管理器在对命令进行接收的同时，也要对命令接收的正确性做出判断。这种判断只是针对在传输过程中可能产生的错误而言的，并不涉及命令的具体内容，因此通常是利用诸如奇偶校验位、校验和等手段来实现。对分组传输协议，则还可以通过判断分组长度的正确与否来实现。当发现命令接收有错后，不同的信息交换协议可能会有不同的处理方法。

如果传送管理器认为对命令的接收是正确的，那么，他将接收到的命令的信息部分传送到下一功能模块，即安全管理器，而滤掉诸如起始位、停止位之类的附加信息。

（2）安全体系（Security Structure）

安全体系在概念上包括三大部分：安全状态（Security Status），安全属性（Security Attributes）以及安全机制（Security Manchanisms）。其中，安全状态是指智能卡在当前所处的一种状态，这种状态是在智能卡进行完复位应答或者是在它处理完某个命令之后得到的。安全属性实际上是定义了执行某个命令所需要的一些条件，只有智能卡满足了这些条件，该命令才是可以执行的。因此，如果将智能卡当前所处的安全状态和某个操作的安全属性相比较，就可以判断出一个命令在当前状态下是否允许执行，从而达到了安全控制的目的。安全机制可以认为是安全状态实现转移所采用的转移方法和手段，通常包括：通行字鉴别、密码鉴别、数据鉴别及数据加密。

安全机制所实现的为如下三个功能：鉴别与核实、数据加密与解密，文件访问的安全控制。下面对其作简单的介绍，文件访问的安全控制是由文件管理器来实现的，所以它的介绍将在文件管理器中给出。

① 鉴别与核实：鉴别是通过智能卡和阅读器双方同时对任意一个相

同的随机数进行某种相同的加密运算，然后判断双方运算结果得以执行来达到验证的目的。核实是通过由用户向智能卡出示只有他本人才知道的通行字 PIN，并有智能卡对该通行字的正确性进行判断来达到验证的目的。这些实际上在前面第三章的“IC 卡的安全性”一节已经作过介绍。

② 密钥管理：为了防止非法用户的窃听和攻击，在智能卡的数据传输过程中对数据进行了加密。加/解密的过程也在前面第三章作过介绍，这里介绍一下 COS 对密钥的管理。

COS 把数据加密时要用的密钥组织在一起，以文件的形式存储起来，称为密钥文件。最简单的密钥文件就是长度为 8 个字节的纪录的集合。其中的纪录头部分存储的就是密钥的属性信息，例如是可以应用于所有应用文件的密钥还是只对应某一应用文件可用的密钥。但是，不论是什么样的密钥文件，作为一个文件本身，COS 都是通过对文件访问的安全控制机制来保证密钥文件的安全性的。

在 IC 卡操作系统中使用 RSA 密钥机制受到了资源的限制，实现非常困难，只有少数的实验算法[17]。

（3） 应用管理器（Application Manager）

应用管理器的主要任务是在于对智能卡接收的命令的可执行性进行判断。可以认为，应用管理器的实现主要是智能卡中的应用软件的安全机制的实现问题。而因为智能卡的各个应用都是以文件的形式存在，所以，应用管理器的本质就是文件访问的安全控制问题。

（4）文件管理器（File Manager）

文件是指关于数据单元或卡中记录的有组织的集合。COS 通过给每种应用建立一个对应文件的方法来实现它对各个应用的存储及管理。因此，COS 的应用文件中存储的都是与应用程序有关的各种数据或纪录。此外，对某些智能卡的 COS，可能还包含有对应用文件进行控制的应用控制文件。

• 文件系统：COS 的文件按照其所处的逻辑层次可以分为三类：主文件（Master File），专用文件（Dedicated File）以及基本文件（Elementary File）。其中，主文件对任何 COS 都是必不可少的，它是包含有文件控制信息及可分配存储区的唯一文件，其作用相当于 COS 文件系统的根文件，处于 COS 文件系统的最高层；基本文件也是必不可少的一个部分，它是实际用来存储各应用的数据单元或纪录的文件，处于文件系统的最低层；

而专用文件是可选的，它存储的主要是文件的控制信息、文件的位置、大小等数据信息。

• 文件访问安全：对文件访问的安全性控制是 COS 系统中的一个十分重要的部分，其实现的方法比较有代表性的方式有：鉴别寄存器方式。

采用鉴别寄存器方式时，通常是在内存 RAM 中设置一个 8 位（或者是 16 位）长的区域作为鉴别用寄存器。这里的鉴别是指对安全控制密码的鉴别。鉴别用寄存器所反映的是智能卡在当前所处的安全状态。采用这种方式时，智能卡的每个文件的文件头中通常都存储有该文件能够被访问的条件，一般是包括读、写两个条件，这就构成了该文件的安全属性。而用户通过向智能卡输入安全密码，就可以改变卡的安全状态，这一过程就是鉴别寄存器方式的安全机制。把三方面结合起来，就能够对卡内的文件的读些权限加以控制了。

5.2　非接触式 CPU 卡

如前所述，由于 CPU 的功耗问题，在非接触式 IC 卡中嵌入 CPU 一直是一个比较困难的事情。但是为了非接触式 IC 卡的发展，人们一直在探索各种各样的解决途径。在不断的研究过程中，这个问题正在一步一步的被解决，从而非接触式的 CPU 卡也慢慢的出现了多种产品。下面就非接触式 CPU 卡的一些实现方法介绍如下。

5.2.1 双界面复合卡—Dualface Card

为了解决非接触式 CPU 卡的能量供给问题，一种折衷的并且是过渡时期的解决办法是将非接触式和接触式 IC 卡结合起来，成为适合两种标准接口界面的 IC 卡。而 CPU 部分的能量供给则由接触式部分提供，这种卡被称为双界面复合卡[21]。

由于 CPU 的能量是由接触式部分提供的，所以实际上该 IC 卡只有在作为接触式卡片使用的时候才能作为 CPU 卡使用。而在非接触式使用状态下，则只能作为逻辑加密卡使用。所以，这种解决方案不能说完全解决了非接触式 IC 卡的 CPU 化的问题。但是，这种卡的出现使得一张卡可以在不同的场合要求下工作，增加了卡应用的灵活性。作为非接触式 IC 卡 CPU 化的过渡产品还是起到了一定的促进作用。

这种双面复合卡的代表有飞利浦公司的 MIFARE® PLUS 双界面卡。

卡芯片的核心部分是一个 8K 字节的 EEPROM。其中存储着应用数据。对 EEPROM 存储器的访问是经过两个完全分离的逻辑结构进行的。如同双端口的 RAM 那样，可以按需要经过两个分别的接口访问。

非接触界面是以 ASIC 为基础的，它完全复制了非接触的 MIFARE® Light 存储卡。于是，从非接触阅读器的观点来看，用 MIFARE® PLUS 双界面卡通信与用普通的非接触 MIFARE® Light 存储卡没有什么不同。另一方面，经过接触界面的通信是经过一个有自己的操作系统的 8051 微处理器进行的。这种界面的结构与微处理器卡相符。

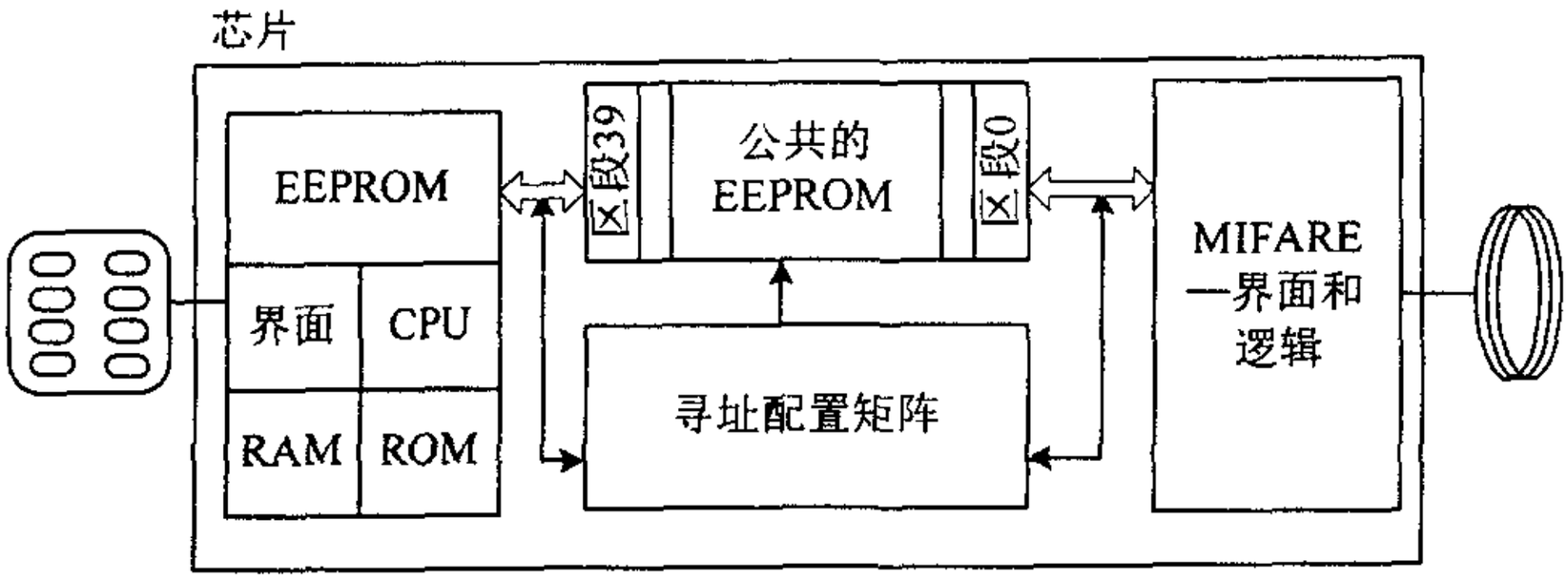


图5.1 MIFARE“双界面卡”芯片的方框图（在非接触操作状态中，经过一个MIFARE相容的状态机访问EEPROM。在经触点操作时，微处理器用自己的操作系统访问同一个存储器）

经两种界面对 EEPROM 的访问权由访问配置矩阵管理。对于两种界面，访问配置矩阵可以把单独的访问权分配到选定的存储区。这样，就可以容许使用分级安全概念。

虽然这种解决方法是一种过渡产品，但是人们却从中发现了这种双界面卡的好处。因为虽然非接触式卡较接触式卡有很多的优点，但是，由于现在接触式卡的数量较多，所以有很多的接触式阅读器设备。双面卡可以对以往的设备兼容，这样资金的投入可以缩减，就好像 IC 卡在标准中也保留了对磁卡和条码卡兼容的设置。另外，在一些操作时间要求不高，而在要求反复读写卡片的场所，接触式 IC 卡反而具有更方便的优势。总之，双面卡技术提供了一种更为灵活的方式来实现一卡化的工作，而使得对阅读器的限制减少了[21]。因此，在即使出现了带有微处理器的非接触式 IC 卡的产品时，仍然出现了另外一种双界面卡，这是双界面卡的进一步发展。

这种思想的基础是智能卡的界面和逻辑之间完全独立。界面形成了应

用的最下层。对数据传输来说是透明的，这意味着从应用软件的观点来看与使用何种界面是不相干的。界面可按意愿予以改变，界面和逻辑部件可以任意组合。对使用者和系统操作人员来说，这种双界面卡的最大好处是：在引入新的应用时可任意选用已经存在的基础设施。

触点和高频界面之间的转接可通过微处理器的操作系统或通过芯片上附加的开关矩阵来完成。

用开关矩阵自动转接时，由来自高频界面或触点馈给的供电电压作为选择标准。当卡插入到接触式阅读器时或在接近非接触阅读器时，由首先给芯片供应的电源选择界面，另一个界面则完全去活化。所以，经过两个界面同时操作是不可能的。自动换接的另一种可能方法是测定时钟信号是经过高频界面还是由触点提供给芯片的。

用操作系统本身执行转接时，以经一个或两个接口收到的数据的有效性作为选择的标准。

这种双界面卡的代表有 Philips 公司的 Mifare® PRO 双界面卡。它包括有一个高速的 triple – DES（3 - DES）协处理器，并且两个界面都能满足世界金融业的安全要求，而非接触式界面则可以提供公共交通运输所需要的快捷和方便[43]。

5.2.2 非接触式 CPU 卡

当今非接触式 CPU 卡的种类还不多，这是由于所需要的技术还不是很成熟。从前面第二章的叙述中可以得知，为了给微处理器提供足够高的时钟频率，需要 IC 卡的系统工作频率在 13.56MHz 以上。而在高频系统中能量的作用距离随着工作频率的增加而逐渐减小（见图 5.2）[2]。所以，在一定的作用距离的要求下，要兼顾微处理器的运算速度和能量的供给，则必须选择合适的频率。近耦合 IC 卡标准选择工作频率为 13.56MHz，也是考虑到了这一问题。

为了给非接触式 IC 卡片内的微处理器提供足够的工作电压（也就是提供足够的射频能量），一般可以通过两种途径进行解决。一种是通过降低片内微处理器的额定功耗和工作电压（故现在多采用 CMOS 技术），这需要微处理器技术和新型集成电路技术的支持。另一种则是加强阅读器的场强和输出功率，这可以通过增大阅读器的天线面积或者调整应答器的等效阻抗来实现。显然，后一种方法较为实际，所以，现在的厂商大多采用后一种方法。

非接触式微处理器卡的出现已经引起了广大智能卡生产商的注意，有一些大公司开始推出了各自的非接触式 CPU 卡的产品，如 Motorola 就曾推出了 Jupiter 系列，其中的 MV3000L 则是一款带有 8 位微处理器的非接触式 IC 卡，其 ROM 的容量为 22KB，带有 512B 的 RAM 和最多 8KB 的 EEPROM，接口界面符合 ISO 14443 Type B 标准[18]。Philips 也将推出 MIFARE® PROX。其包含有 Philips 的 FameX 加/解密协处理器，可以在非接触式的智能卡上实现高保密性能的公开密钥数据加密体制（如 RSA）[43]。

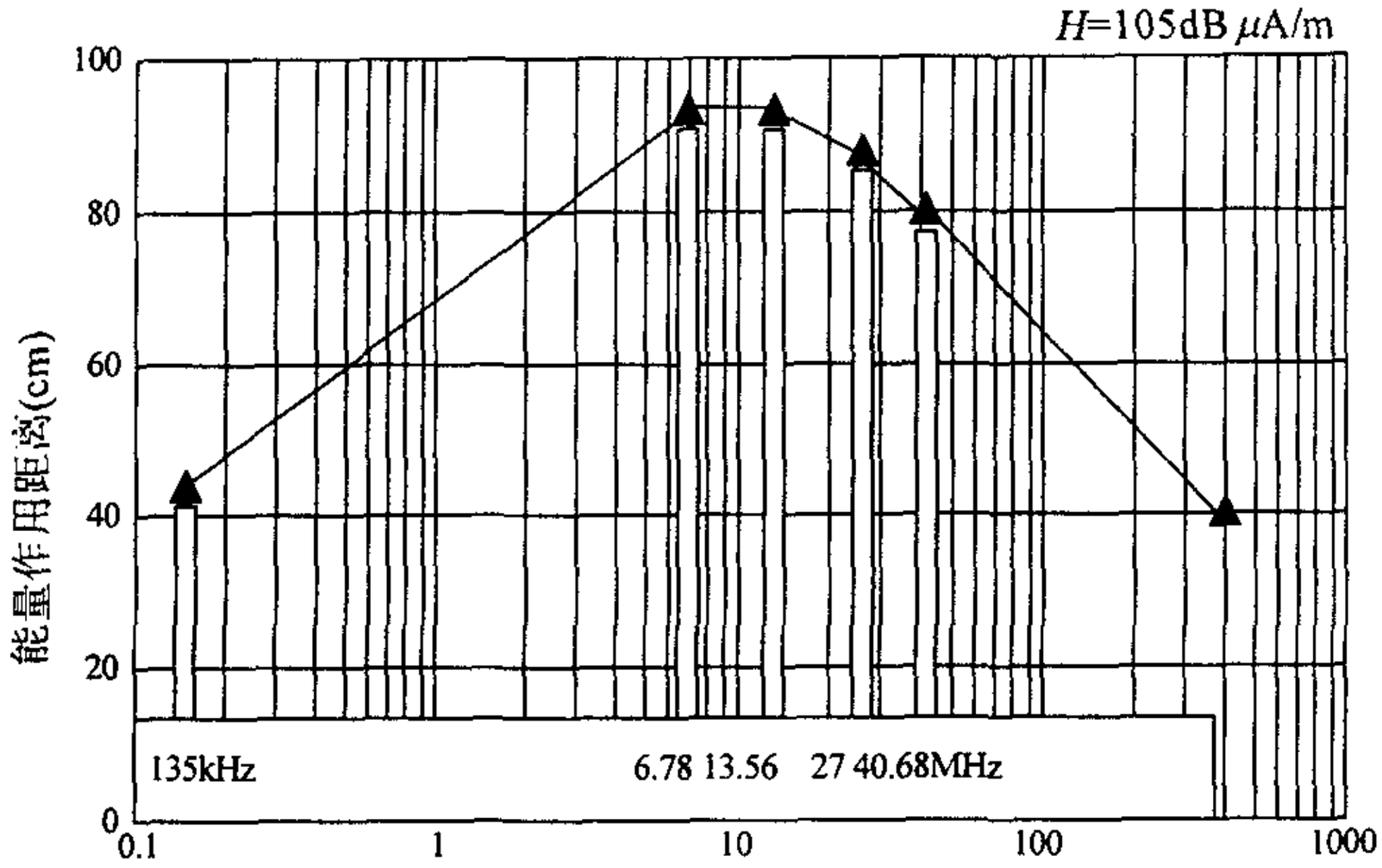


图5.2 相同场强时应答器的作用距离（在阅读器天线面积和阅读器天线磁场强度不变的情况下，测量应答器上的感应电压）

第六章　非接触式 IC 卡的应用

非接触式 IC 卡应用潜力最大的领域之一就是公共交通领域。在欧洲和美国，各交通联合体同以往一样赤字高悬，部分甚至达到了营业额的 40%[2]，在中国的各大城市公共交通情况也好不到哪儿去。公交公司摆脱亏损一直是个非常重要也非常艰巨的问题。由于调控手段越来越有限，必须要从长远打算，寻找出增收节支的扭亏方案。使用非接触式 IC 卡作为电子车票（AFC: automatic fare collection）能够为改善这种局面作出非常重要的贡献。

6.1 公共交通对电子车票的需求——市场需求分析

公共交通企业面临的糟糕的财政形势是有多方面原因的。其中一些促使了公共交通企业对电子车票的需求：

- 纸制的车票用过后就会被丢弃掉，对于交通企业来说生产防伪车票的开支越来越大。
- 企业的结算只能根据花费高昂的抽样计数来进行，而它又使结算不精确。
- 使用无人售票的车辆，车票的发售需由司机负责，这样在乘客上车时就会出现较长的一段停车时间，这还不算由于司机经常分散注意力而产生的附加的安全风险。
- 另外，还必须算上由于逃票、假币或者残币带来的高额的票款损失。

因此，对于电子车票管理人们有很大的期望和要求，特别是考虑到它不受气候影响、无磨损、读写速度快以及操作便利等特点。这些期望只能利用射频识别系统才能真正满意地加以实现。作为结构形式，则首先会采用具有 ID－1 结构的非接触式 IC 卡。

1. 交易时间：公共交通对电子票务管理最大最关键的要求，就是购票及检票所耗费的时间了。对于交通工具，只有在车厢内才能进行检票。这个问题通常会出现在公共汽车和城市有轨电车上。对于地铁还可以在中转站或通过流动检票员来进行检票。而非接触式 IC 卡系统在时间上有着明

显的优势，这是使用接触式 IC 卡或现金所无法比拟的优势。

2. 天气适用性，使用寿命，操作便利性：非接触式 IC 卡的设计使用寿命为 10 年。下雨、寒冷、暑热、脏污及灰尘既不会对 IC 卡也不会对读取设备构成损害。非接触式 IC 卡也可以放置在信封或手包内，使用非常方便。

3. 使用射频识别系统的优势：采用基于非接触式 IC 卡技术的现代化的电子车票管理方式来取代传统的纸质车票会给各个方面带来许多好处。一套非接触式 IC 卡系统的购置价格目前虽然比一套传统系统还是要高些，但所付出的投资在短时间内就可收回。

6.2　系统的组成

由上述可知，公共交通领域对射频 IC 卡系统的需求很大的，特别是近几年以来，在我国的各大城市中已经有越来越多的公交公司实现了电子车票系统。这两年株洲和长沙两地也相继开始采用公交电子车票系统。本文就以株洲市公交公司的射频IC卡系统为例阐述非接触式IC卡是怎样应用在公共交通领域的。

从一张非接触式 IC 卡所经历的流程来看，一张卡必须经过初始化、发卡、使用和再充值等几个环节[26]。在不同的环节中，需要由不同的卡片读写机来对卡进行处理。所以系统首先需要由 IC 卡读写器（实现卡片的初始化）、充值机（发卡和对卡片充值）和车载机（与卡片进行交易）来完成对卡片的操作。

而在整个系统中最重要的是数据的流程，其中需要对各单笔交易的数据汇总，然后再传送给各车队，再由各车队将数据传送到所属的分公司再汇总，最后送到结算中心或者总公司汇总。所以各车队、分公司和总公司及结算中心的数据网络建设是必需的，而从各车载机到车队之间的数据传递则由数据采集机来完成[29]。

由此可见，整个系统的硬件组成需要由射频 IC 卡、IC 卡读写器、充值机、车载机、数据采集机以及数据通信网和相应的微机构成。其中射频 IC 卡又分为乘车卡、司机卡和管理卡三类，以满足管理和安全的要求。而软件系统则需要由数据库系统、数据通信系统以及数据操作系统三个部分组成。另外，由于要实现的是金融数据的处理，所以安全系统也是必不

可少的一环，以保护公交公司和乘客的合法利益，安全系统则通过硬件和软件两个方面进行实现。

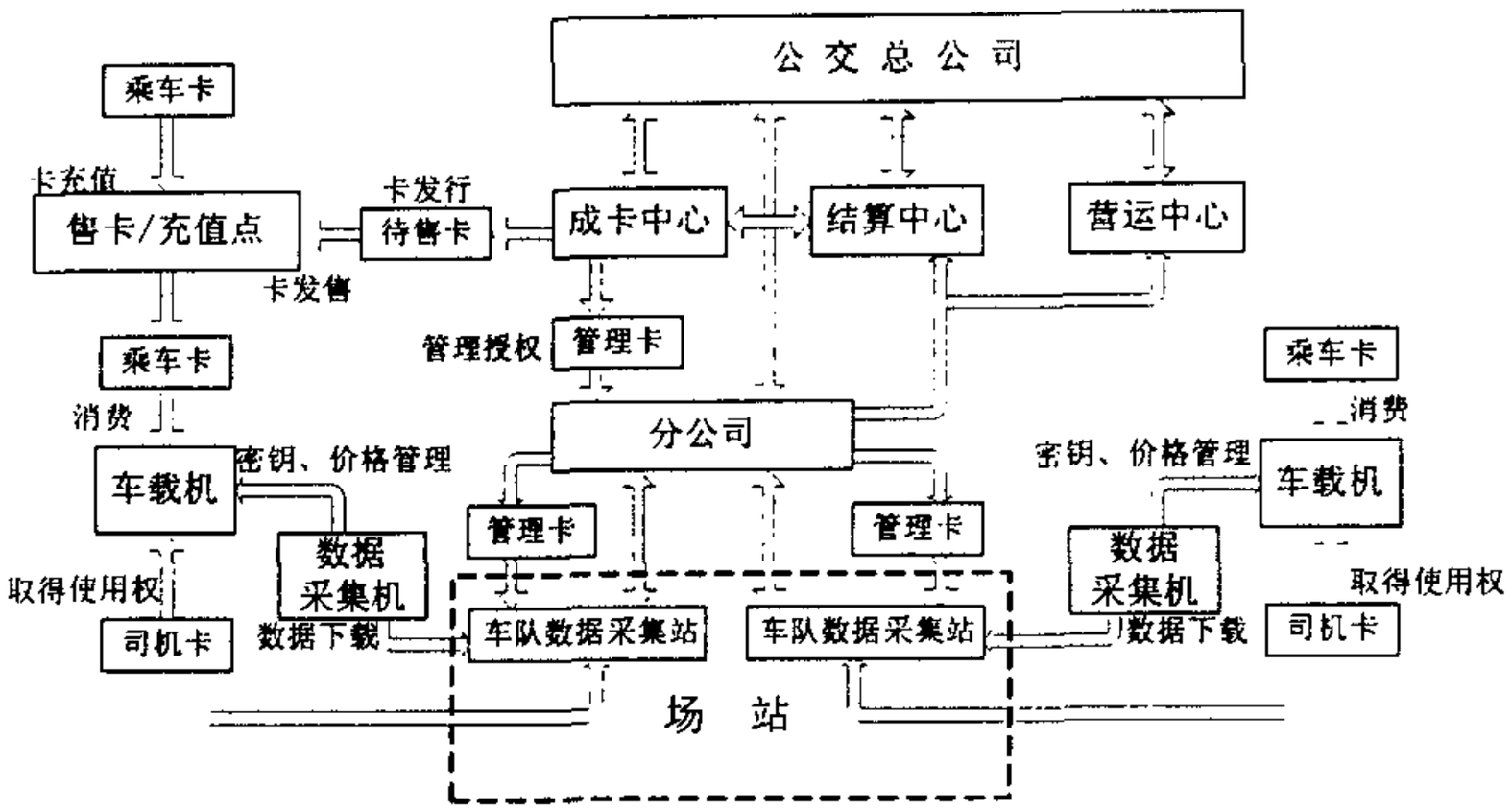


图6.1 系统的组成

图 6.1 将系统的组成和数据及 IC 卡的流程清楚地显示出来。

6.3 系统管理体系及安全策略设计

从系统的核心职能来看，主要是对公交营运的数据进行处理。可以将其分为数据的访问和数据的传输两个方面，从这两个方面入手，对系统的管理体系和安全策略可以分为数据访问控制和数据流向控制两个子系统。另外，对于非法数据的侵入，也是安全策略设计所必须考虑的问题。

6.3.1 数据访问控制

系统的数据可分为原始数据和统计数据两类，原始数据储存在射频 IC 卡和射频 IC 卡读写机具中，特别是乘车卡和车载机中存储的是最有意义的交易数据。而统计数据则存储在各数据采集站和分公司、总公司以及各充值点的微机中。所以数据访问控制则包括对射频 IC 卡、读写机具的访问和对这些微机的访问控制。

1．对射频 IC 卡的访问控制。

对射频 IC 卡中的数据进行访问，实际上就是对射频 IC 卡的存储器进行访问。访问可以分为读、写以及增、减等操作。为了保证对卡的合法操作以及乘客和公交公司的合法利益，对卡内存储器的操作必须由具有授权

的射频 IC 卡读写器进行。在读写机具对射频 IC 卡进行操作之前，首先须进行相互的认证，以便确定读写机具和射频 IC 卡是否合法。之后，读写机具在对射频 IC 卡的某个存储区域进行访问的时候，也必须具有相应的权限（安全状态符合安全属性）才能对该存储区域进行操作。这些将在后面的硬件设计中详述。另外，其中数据加密采用的是 3－DES 算法。

2．对读写机具的访问控制。

由于读写机具是对射频 IC 卡进行操作的直接设备，所以为了防止对卡内数据随意的或人为的非法修改，读写机具的管理对系统的安全性的影响也是非常重要的。同时，读写机具对卡数据操作的详细情况也需要有所记录以便和卡内纪录的改变作为相互核对的依据。

为了明晰管理权限，对每一台读写机具的操作都必须由专门的操作员来执行。而操作员为了证明自己的身份，必须拥有自己的 PIN 和相应读写机具的操作管理卡。正如前面所提及，系统中的射频 IC 卡分为乘车卡、司机卡和管理卡，操作员所拥有的则是管理卡。在操作读写机具之前，操作员首先用操作卡开启读写机具。读写机具则会要求操作员在终端或者 POS 中输入自己的 PIN，并将其与操作卡中存储的 PIN 进行认证。在确认为合法的操作员之后才能对读写机具进行操作，而操作期间的所有记录则存入到该操作员的考勤统计数据中去。操作员在下班前也需要使用操作卡关闭读写机具，以便正确的统计各操作员的考勤记录。

所有的读写机具如发卡机、充值机、以及车载机等都需要按照上述方法访问。其中应该指出的是车载机比较特殊，因为其安装的位置是在汽车上，不像别的读写机具都与终端或者 POS 相连，也不是由专人照管和操作。这时候司机就起到了操作员的作用，而司机卡也可以认为是车载机的操作卡。可以在车载机上安装小键盘，以便司机进行 PIN 认证。

另外，由于数据采集器需要对车载机进行访问，所以数据采集员也必须持数据采集卡来启动车载机才能从中将数据下载到数据采集器中。其过程与上述过程类似。

3．对微机的访问控制。

对于微机的访问则主要靠操作系统和应用软件的用户权限控制来实现。

6.3.2 数据流向控制

数据的流向可以分为上行和下行。上行指的是乘车卡的原始数据从被

采集到汇总的流动过程，下行则是指由总公司下达的行政指令和营运参数调整指令的流向。以乘车卡中的原始数据的流动程序可以对数据流向控制进行设计。

1．卡的初始化：白卡是指来自卡片制造商处未经过处理的卡片，卡中只带有全世界唯一的卡号及制造商的密钥。所以白卡在发行之前需要对卡内的存储区划分应用区域——即卡的格式化，以及写入发卡方的数据。同时为了系统的安全保障，需要在建立主文件和应用数据文件的同时确定对记录文件的操作权限[30]。在白卡格式化的过程中，所需要做的事情主要是把制造商的密钥替换为公交公司自己的密钥，然后在卡的存储区内划分好主文件（MF），对主文件指定操作权限密钥；然后在主文件密钥的权限下建立公交电子车票应用的应用目录文件以及应用文件，这些文件包括有个人档案文件、标志文件（如挂失记录允许标志、优惠比例等）、电子钱包文件、充值记录文件及流水记录文件等等。这些文件也有各自的权限密钥保护，来控制外界对卡上存储区的读写。这些操作需要在公交总公司成卡中心内拥有最高权限的读写机具上进行。

2．卡的发行：卡的发行是在各 IC 卡发售点进行的，在这所需要进行的操作就是在相应的权限下对卡中公交电子车票应用存储区的应用文件中写入初始纪录。如对个人档案文件中写入乘客或司机（司机卡）、管理员（管理卡）的信息，以及在电子钱包文件中写入初始存入的金额等。

3．卡的交易：乘车卡在使用时与车载机进行通信。在交易开始之前首先要进行车载机和乘车卡的相互认证，只有在认证通过之后车载机才能对 IC 卡的电子钱包文件进行改写，扣除乘车的费用。另外，在乘车卡的流水记录文件中将写入该次交易的时间、路线、车号以及交易金额等信息。在这个过程中车载机始终拥有对上述文件的读或写的权限。

4．卡的再充值：同样是在各充值点的充值机上，在拥有相应的权限的情况下对 IC 卡的电子车票文件改写，加上充入的金额数目。同时，还要在乘车卡中的充值记录文件中写入相应的纪录。

5．上行数据流向控制：由数据采集员使用数据采集器将各车载机中的数据下载到各数据采集站中，在通过数据通信网络一级一级上传和汇总，直到总公司和结算中心。

6．下行数据流向控制：总公司的行政命令可以由数据网络进行下达，而牵涉到修改射频 IC 卡内营运参数（如票价、路线等）的操作则需要使

用行政管理卡对下级读写机具授权，其过程如前数据访问控制中所述。

6.3.3 非法数据的处理

系统在运行的过程中不可避免地要受到来自不同方面的入侵，有些是无意的，有些是人为的。其中主要的入侵就是非法数据，这就要求系统能够辨认有效的数据以保障公交公司和乘客的合法利益。

非法数据的表现形式多为非法的乘车卡，如卡中金额已透支、已挂失卡以及假卡等。另外，也有假冒射频 IC 卡读写机具对射频 IC 卡进行非法充值等情况。前面所述的读写机具和卡的访问控制中可以解决其中的部分问题，如卡与读写机具的相互认证可以减少非法卡和非法读写机具对系统攻击的成功率[27]。

另外，为了防止失效卡、已透支卡和非法卡对系统造成损失，须对这些非法的数据进行处理。可以引入黑名单概念以标识这些非法数据，使得读写机具能够识别有效的数据[28]。当非法数据出现在系统的任何一个读写机具处时，读写机具在报警的同时将卡序列号、发行号等进行纪录，并在卡内的黑名单标志处进行标记。每一天的数据汇总之后，将所有的黑名单进行统计并将结果发送给各车队，第二天由数据采集器将黑名单上传给各车载机。而车载机在进行交易之前首先则检查乘车卡的卡号是否在黑名单中，以确定乘车卡的合法性。这样，就将非法数据可能造成的损害限制在最多一天的时间以内（因为车载机的脱机工作特性限制）。

6.4 系统的硬件设计

在确定了系统的安全策略和数据的流程之后，就要开始对系统进行硬件设计了。系统的硬件设计包括非接触 IC 卡的选型、应用文件结构设计等；非接触 IC 卡读写机具（包括充值机、车载机等）设计；网络拓扑结构设计和网络的构建等方面的硬件设计工作。

6.4.1 射频 IC 卡的设计

因为系统所要实现的主要功能就是对射频 IC 卡的操作，所以射频 IC 卡的设计对系统来说具有决定性的意义。只有在选定了使用卡的类型之后，才能对读写机具进行具体的设计工作。通过对系统的规模、性价比，以及系统的功能要求的综合考虑。最终选定了飞利浦公司生产的 MIFARE® MF1 型逻辑加密射频 IC 卡。该卡的操作距离可达到 10cm；典

型的交易时间（包括备份管理）小于 100ms；拥有 1Kbytes 的 EEPROM 存储区，分为 16 个扇区，每个扇区分为 4 个 16 字节的块；每个扇区都有两个可由用户设计的密钥保护，适于多应用的设计；安全上则采用了 3－PASS 认证、流密钥等技术，对于在公共交通领域在操作速度、存储容量以及其金融交易安全性的要求是完全能够满足的。并且还可以支持多应用系统的扩展，对于公共交通领域在其他范围如地铁方面的使用提供便利。

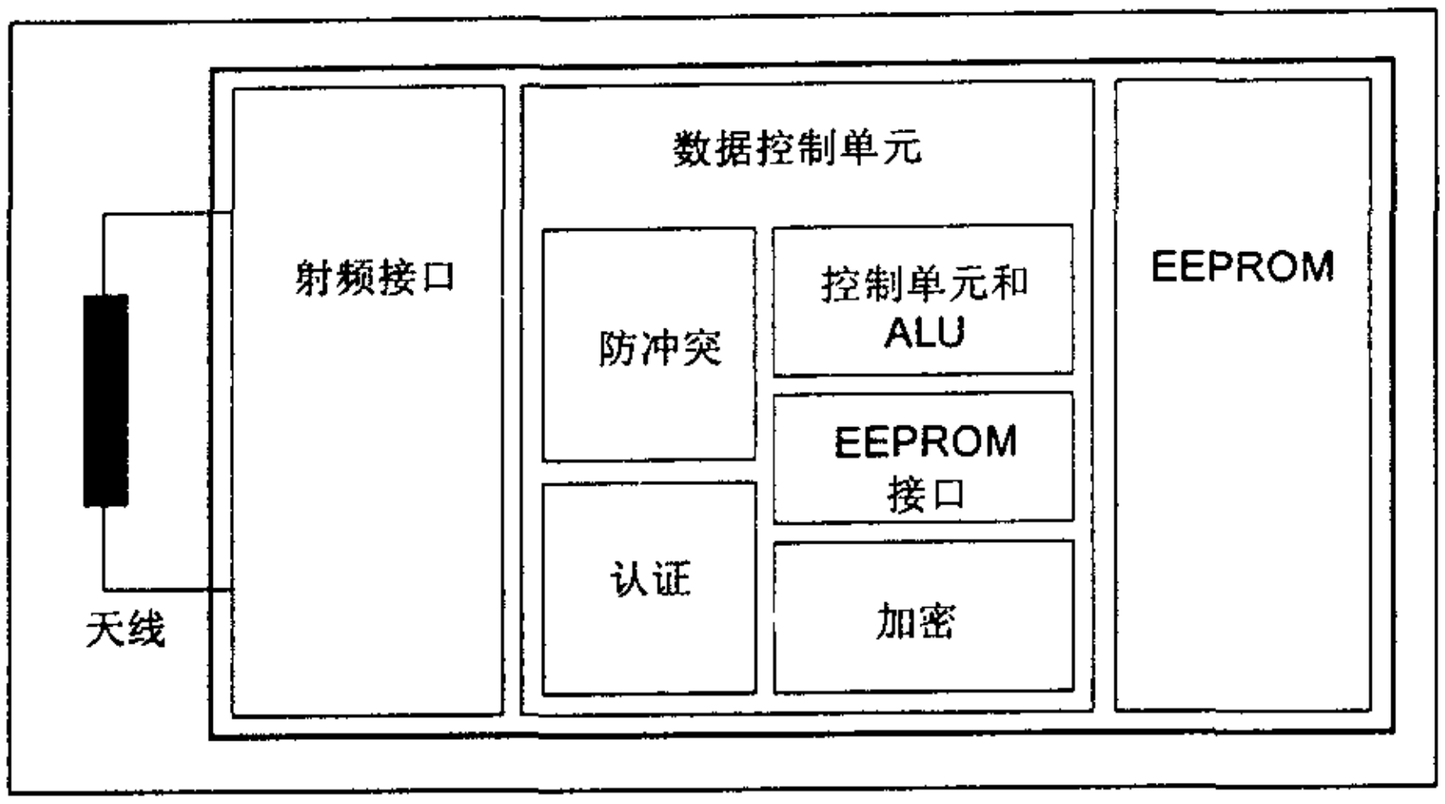


图6.2 MF1型射频C卡的结构

MF1 型射频 IC 卡为逻辑加密卡，符合 ISO14443 TypeA 型卡标准，主要由射频天线和 MF1 芯片构成而不需要其他的辅助电路。MF1 芯片由射频接口、数据控制单元和 EEPROM 组成，其结构如图 6.2 所示[44]。

MF1 芯片的 EEPROM 如前所述分为 16 个扇区，并且符合在第三章中所述的 MIFARE®智能卡应用目录的格式。每个扇区的第四个块（Block3）被称为扇区尾（Sector Trailer），另外的三个块为数据块可用于应用数据或者控制数据的存储区。数据块可能可以执行读（read）、写（write）、增（increment）、减（decrement）、恢复（restore）或移动（transfer）等操作，而这些操作的允许与否则由扇区尾的记录所确定[22]。每一张 MF1 卡的 0 扇区 0 块都存放有唯一的序列号，被称为生产商块，该块不受扇区尾的控制，在卡片生产之后就被设置为只读且不能被改变。

扇区尾由密钥 A、密钥 B 和访问条件位（Access Bits）三部分组成，其中密钥 B 是可选的。密钥 A 和 B 占用头和尾各六个字节，访问条件占用扇区尾的第 6 到第 9 共 4 个字节。访问条件位控制着该扇区中所有块的

操作权限——即访问条件（Access Condition）[44]。访问条件中每三位的值对应着一个块的访问条件，这个访问条件位确定对该块的访问是可读、写或是其他的操作，并确定该操作是在密钥 A 还是密钥 B 的控制下进行，如图 6.3 所示。在所有的对存储器的操作之前都必须先使用密钥 A 进行 3 - PASS 认证，然后在密钥 A 的控制之下才能对卡内的存储器进行相应的读、写等操作。因此，白卡的初始化最开始就必须将需要使用的块内的密钥 A 替换为发行商自己的密钥，然后才能对存储器进行划分。

Access Bits	Valid Commands		Block	Description
$C1_3\ C2_3\ C3_3$	read, write	→	3	sector trailer
$C1_2\ C2_2\ C3_2$	read, write, increment, decrement, transfer, restore	→	2	data block
$C1_1\ C2_1\ C3_1$	read, write, increment, decrement, transfer, restore	→	1	data block
$C1_0\ C2_0\ C3_0$	read, write, increment, decrement, transfer, restore	→	0	data block

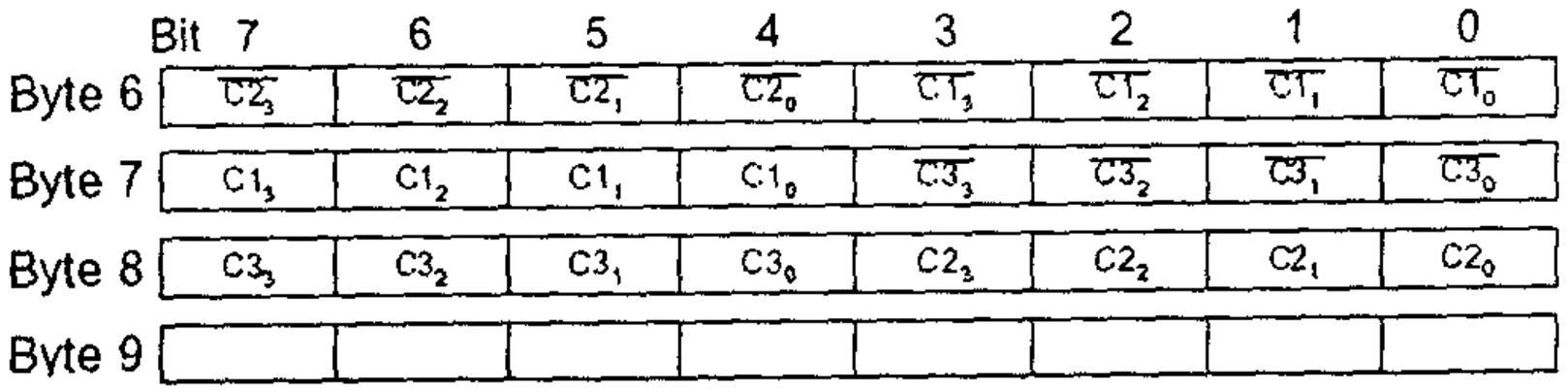


图6.3 访问控制位的组成控制位所对应的块

对存储器划分为应用文件，需要对该应用的文件系统进行设计。卡内存储器的 0 扇区保存有卡的唯一标志号，虽然余下的数据块可以使用，但是一般都不把应用文件建立在该扇区之中[9]。而将主文件（MF）以及主目录文件建立在该扇区下。另外的 15 个扇区可以作为应用文件的存储区，每个扇区都可以作为一个独立应用的存储区，所以理论上一张 MF1 卡可以执行 15 种应用。对于公交系统来说，需要建立有关于发行、充值、交易等信息的文件，所以需要占用多个扇区，对存储区的划分设计如图 6.4 所示。

扇区	块	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0 应用标识目录区	0	唯一序列号（CSN）															
	1																
	2																
	3	Key A0						Access Bits				Key B0					

1 发行区	0	城市代码		行业代码		发行流水好		卡认证码			启用标志	卡类	押金		
	1	发行日期				有效期		启用日期			加款POS号				
	2	加款时间				原额 1		本次加款		余额				操作	
	3	Key A1					Access Bits			Key B1					
2 钱包区	0	透支额度				累计加款值									
	1	钱包				钱包		钱包			最大值				
	2	钱包备份				钱包备份		钱包备份			最大值备份				
	3	Key A2					Access Bits			Key B2					
3 钱包交易记录区A	0	交易时间 日/时/分/秒				原额		交易金额		交易类型	POS号 版本号				
	1														
	2														
	3	Key A3					Access Bits			Key B3					
4 钱包交易记录区B	0	交易时间 日/时/分/秒				原额		交易金额		交易类型	POS号				
	1														
	2														
	3	Key A4					Access Bits			Key B4					
5 公共信息区	0	钱包交易指针		钱包累计交易次数		交易类型	月票累计交易次数		黑名单标志						
	1														
	2														
	3	Key A5					Access Bits			Key B5					
6 月票文件	0	金额/次				购买日期									
	1	月票计数器				月票计数器		月票计数器			年/月				
	2	月票计数器				月票计数器		月票计数器			年/月				
	3	Key A7					Access Bits			Key B7					

图6.4　卡内存储器文件结构组成

6.4.2 射频 IC 卡读写机具的设计

系统另外一个使用最多的就是射频 IC 卡的读写机具了，所有直接对射频 IC 卡进行操作的设备都是射频 IC 卡读写机具。而由于使用的都是同一种型号的射频 IC 卡，所以射频 IC 卡读写机具的核心部分都是相同的，它主要包括读写器的射频接口、控制电路和通讯接口等。由于硬件部分对周围环境的影响比较敏感，所以在设计的时候还必须考虑到读写器的工作环境。特别是车载机，由于是在行驶中的公共交通工具上使用，灰尘、电磁脉冲、无线电干扰都比较大，如何克服这些影响而正常工作都是必须解决的问题。

以车载机为例，射频 IC 卡读写器的电路由射频接口电路、微处理器、存储器、通讯电路、显示电路以及一些辅助电路组成，如图 6.5 所示。其中的 Reader ASIC 为射频读写集成电路芯片，采用的是 MIFARE® MF CM200 模块。该模块的射频部分与天线面板接口，而在逻辑电路部分拥有与 8 位微处理器总线的接口。并能够实现如调制解调、射频信号发生、反碰撞和安全管理的基本功能。使用 5V，40mA 电源供给，为 2×16 的引脚排列，可以作为微处理器的外部设备通过并行控制接口相连[46]。

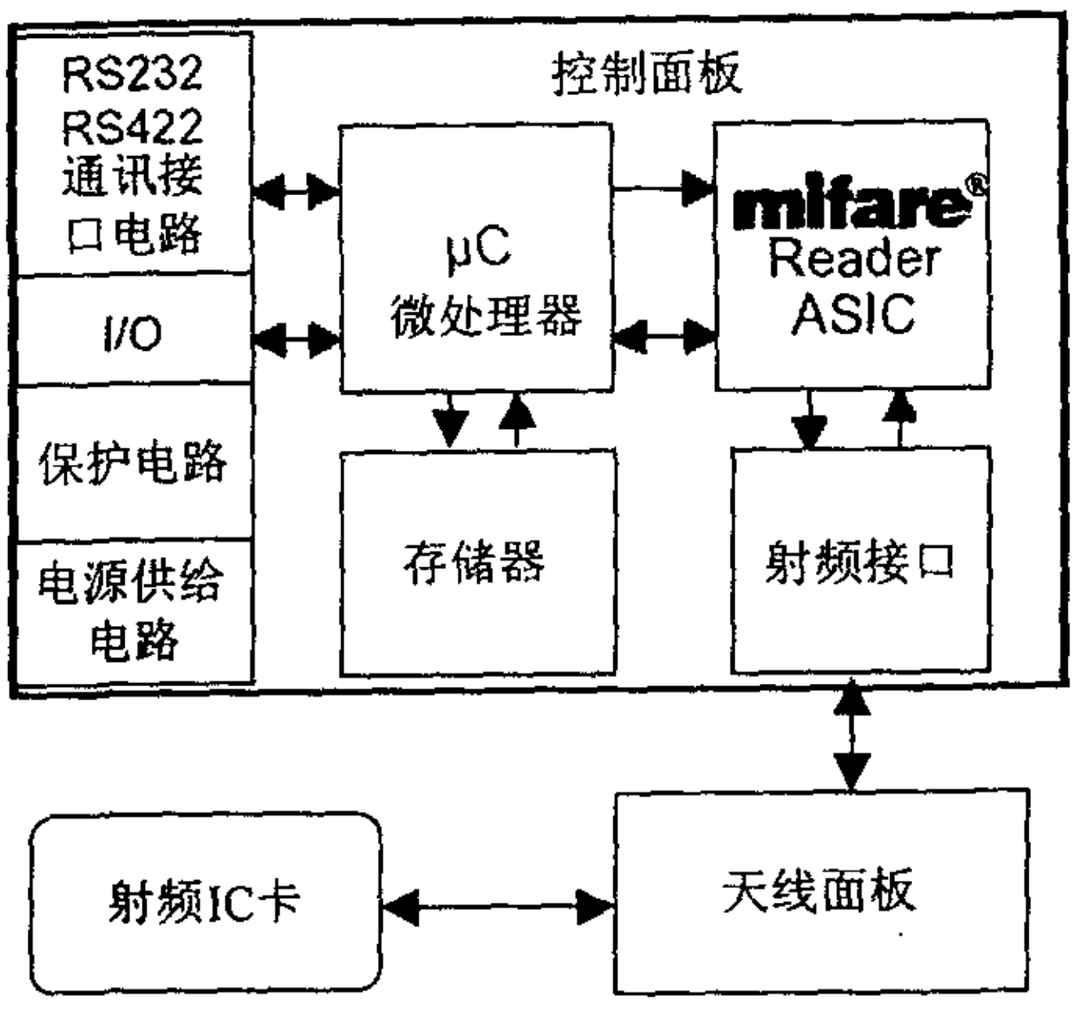


图6.5 射频IC卡读写器的组成模块

微处理器选择的是 51 系列的 ATMEL 公司生产的 AT89C52 单片机，

AT89C52 拥有 8K 字节的 FPEROM（Flash Programmable and Erasable Read Only Memory），已经能够满足车载机程序对存储空间的要求。同时存储器也是采用的 ATMEL 公司的 AT24C256 型 EEPROM。AT24C256 提供 256K 字节的存储容量，车载机采用了一片 AT24C256 作为存储交易记录的存储器，从片中的 100H 处开始存储明细记录数据，以 16 个字节一条记录（包括交易卡发行号、交易时间、交易金额、营运记录号以及标志位等）来计算，可以存储达一万六千多条记录，已经足够存储一辆车一天的交易量。片内的数据结构如图 6.6 所示。

为了适应车辆上较为恶劣的环境，特别是车辆启动时的火花塞产生的高频干扰信号的影响，在读写模块和微处理器之间还必须加上滤波电路，以便保证接收数据的正确性。另外在外壳的设计上则多采用金属屏蔽的方法减弱外来的干扰信号。而在电路的设计上尽量简化布线的布局和减少元器件（特别是储能元件）的使用，则更进一步的降低了硬件部分对外界干扰的敏感程度，从而加强系统的稳定性。

10H:

卡编号	33H	收款员编号	00	CRC8
3字节	1字节	2字节	1字节	

18H:

卡编号	44H	车号	票价	CRC8
3字节	1字节	2字节	1字节	

20H-2FH 同 10H-1FH

司机统计数据区：

40H:

卡编号	司机编号	数据明细首址	末址	人次	金额	CRC16
3字节	2字节	2字节	2字节	2字节	3字节	

50H-5FH 同 40H-4FH

100H:

卡序列号	交易金额	卡中余额	用卡计数	卡编号	打折系数	99H	CRC16
4字节	1字节	2字节	2字节	3字节	1字节		

图6.6 车载机存储器内的数据结构

6.4.3 其他设备的设计

除了射频 IC 卡读写机具之外，还有用于数据采集的数据采集器。数据采集器的设计比较简单，主要部分就是微处理器和较为大容量的存储器。可以通过 RS232 接口与车载机相连，然后在数据采集卡的控制下与车载机通信，将车载机中的数据全部下载到内部的存储器中。然后再将采集到的数据（通常是好几台车载机的数据）也通过 RS232 接口送到车队

数据采集站的终端中。

各数据采集站和汇总中心需要配置若干台 PC 作为终端或数据库服务器，各级车队、公交子公司和总公司之间通过调制解调器进行点对点拨号的方式传送数据。

6.4.4 系统安全策略的硬件实现

大部分的安全策略工作如数据的访问控制是由射频 IC 卡的硬件特性来完成的，正如前面 MF1 卡的数据存储器结构所提供的安全访问机制一样。另外，卡片与读写机具的 3 – pass 认证以及数据加密则主要是由软件实现的（读写机具一端）。

对于黑名单的处理，在 MF1 卡的 5 扇区（公共信息区）划分了一个黑名单标志纪录，以标志该卡的黑名单属性。另外，在车载机中有一片 AT24C64 用于存储黑名单，在设计上，使用该存储器的第 n 位代表发行号为 n 的乘车卡，这样，车载机只要在交易前读出卡片的发行号，就可以找到该位以确认该卡是否为非法卡。一片 AT24C64 有 64K 的存储空间，也就是对应于大约 50 多万张卡片，并且在设计的时候已经留下了备用的 AT24C64 的插槽（已布好线），可以随时将系统扩展到 100 多万的发卡量。

6.5 系统的软件设计

软件的设计相对于硬件设计来说就要复杂得多了，它包括了各读写机具内的软件设计、数据网络各终端的应用软件设计以及数据库的库结构设计等等工作。并且系统大部分功能的实现需要通过软件来实现的，如果说硬件设计保障系统的稳定，那么软件设计的成功与否是整个系统是否能够正常工作和便于扩展的关键。

6.5.1 读写机具的软件设计

和硬件设计一样，直接实现射频 IC 卡读写操作的读写机具的软件设计是最重要的部分。这一部分的软件必须实现对非接触式 IC 卡的相互认证、3-DES 加密算法、对射频 IC 卡存储器的读写操作以及监控程序等。

由于射频 IC 卡读写器的微处理器使用的是 AT89C52，为 51 系列的微处理器，所以其软件使用的是 MCS-51 汇编语言。对于不同的射频 IC 卡读写器，其软件所要实现的功能是不同的。如车载机所要做的是在乘车卡中的钱包文件记录中扣除乘车的费用；充值机则是在乘车卡的钱包文件

中充入金额。或者，对于不同的非接触式 IC 卡，同样一台射频 IC 卡读写器也要执行不同的操作。如对于司机卡，车载机则要更新纪录并开启或关闭读写乘车卡的功能；而对于数据采集卡，要做的则是将存储在车载机中的数据通过 RS232 接口输送到数据采集器中，并在之后重置记录存储器。但是，在这其中有几个部分是不变的，首先就是射频 IC 卡和读写器之间的相互认证，还有就是对射频 IC 卡存储区的操作。因为不管是什么射频 IC 卡读写器，都是对射频 IC 卡存储器中存储的数据进行读、写或其它的操作，只不过是不同的卡或者读写器对不同的扇区进行处理[6]。

因为车载机和乘车卡之间的交易是系统中发生的最多也是最基本的流程，所以以车载机和乘车卡之间的交易来说明读写机具的软件设计最有实际意义。图 6.7 为车载机与乘车卡交易的软件流程图。

流程中的 3 – pass 认证在第三章中的 IC 卡数据的安全性一节中作过了介绍；选择卡片的过程就是射频 IC 卡的反碰撞过程，如果有多张卡同时出现在读写器的作用范围内时，就有反碰撞程序选择其中的一张卡进行操作；读应用分区表是为将来的多应用扩展所作的准备，多应用分区表存储在射频 IC 卡的 0 扇区之下，用来存储各个应用系统的注册编号和存储扇区的指针，以便找到各个应用系统存储扇区的位置。

其它的读写机具对射频 IC 卡的操作程序流程虽然各有不同，但是主要的部分都包括上图中所示的 3 – pass 认证、存储扇区认证、存储扇区操作等这些步骤。由于射频IC卡读写机具和射频IC卡之间的操作种类繁多，故不再一一赘述。

6.5.2 安全策略的软件实现

对于安全策略中可由软件实现的地方主要是 3 – pass 认证流程和数据加密算法。在流程中 6.7 中可以看到，卡和读写机具之间除了要经过 3 – pass 认证之外，还需要在对特定存储区进行操作的时候进行认证。但是，在这个过程中需要认证的密钥 Key A 或者 Key B 都从来不会进行传输，而是经过象 3 – pass 认证一样的过程来进行认证的。

对非法卡的处理，如前所述，在读出发行扇区用户基本信息之后。读写机具则使用读到的卡片发行号来寻找存储黑名单的存储器中的相应位，如果该位为 1 则表示该卡发行号在黑名单中，为非法卡。为了防止对黑名单存储器的无意修改导致的错误，保留了 CRC 校验位，并在车载机的交易存储器中作了纪录，以便汇总时进行核对。

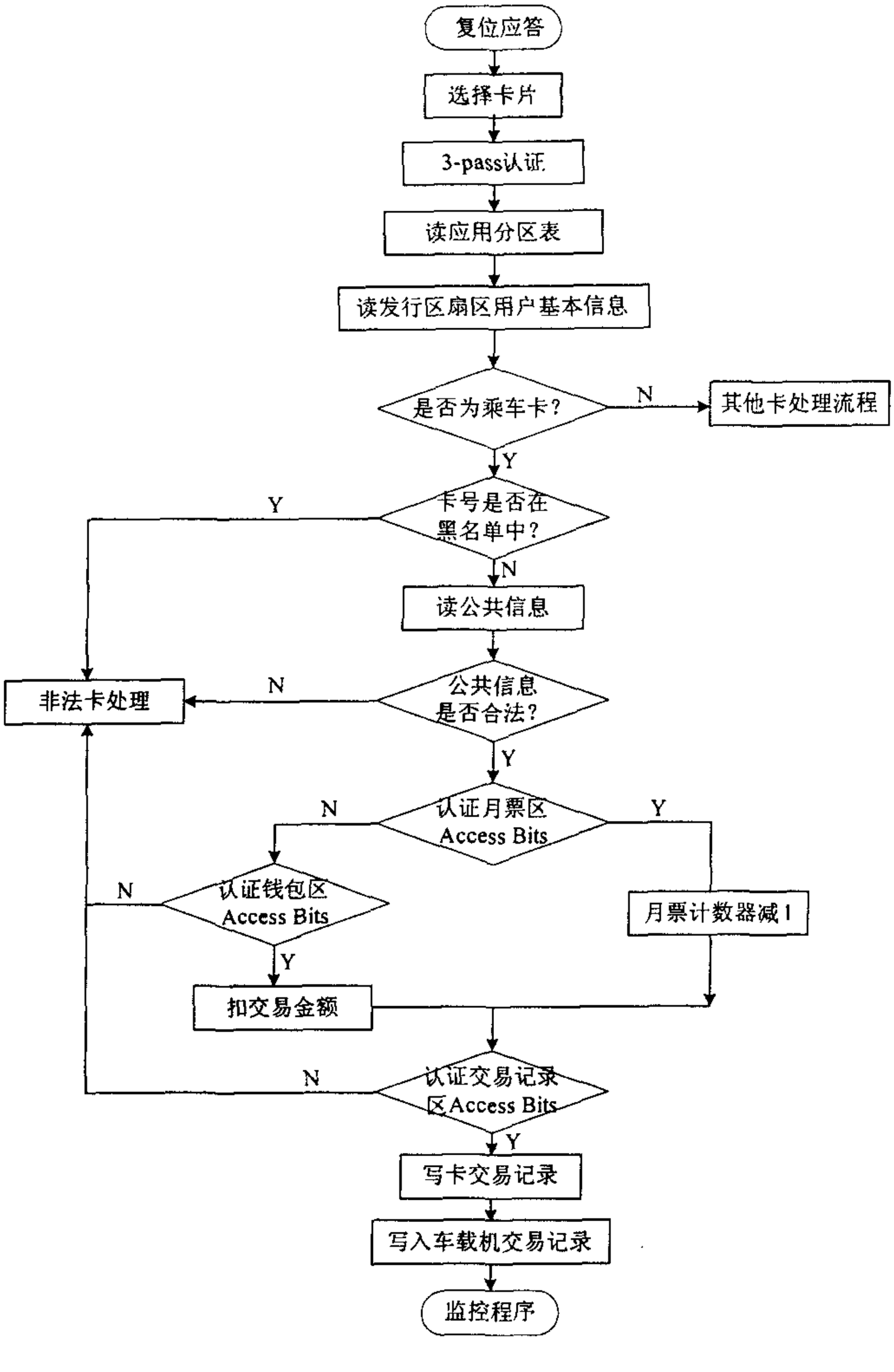


图6.7 车载机与乘车卡交易的程序流程

6.5.3 终端应用程序设计

相对于射频 IC 卡读写机具的程序设计，各数据采集站终端以及发卡、充值中心终端的程序设计可以称为上位机应用程序。因为这部分的应用程序所要完成的任务主要就是与射频 IC 卡读写机具相互通信，读取其中的信息或发送所要执行的射频 IC 卡操作命令。另外一部分任务则是将读取的信息进行处理并通过网络送达上一级的数据中心，并且一般都带有数据库的操作功能，以将收集的数据和操作信息记录备将来的查询核对之用。

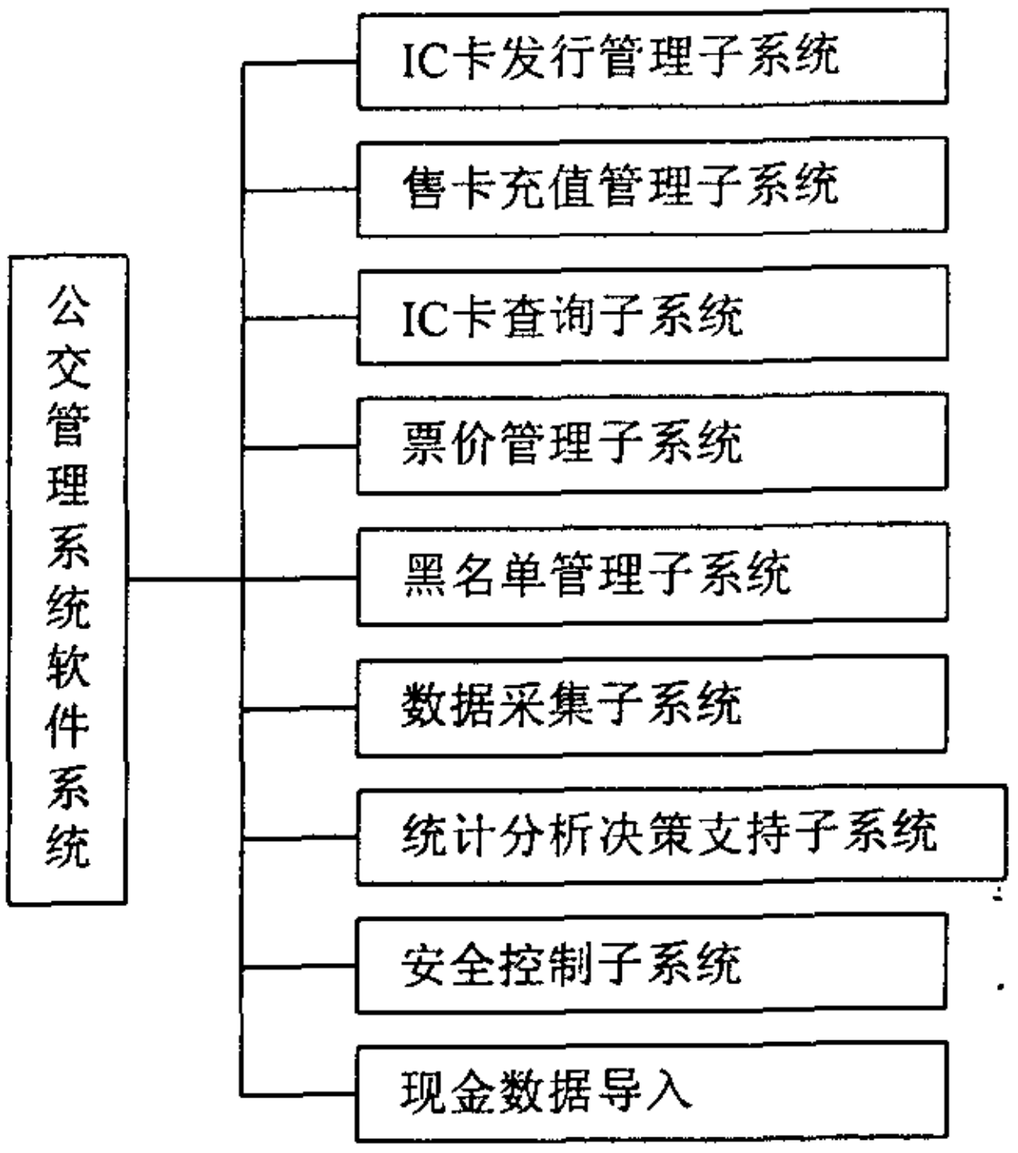


图6.8 上位机应用程序的模块结构

为了确保系统的安全以及数据不被窃取，上位机程序还要求射频 IC 卡读写机具操作员（也就是管理员）确认其身份。在程序启动时，需要管理员用机具操作卡启动读写机具，此时，上位机则要求管理员输入其管理员密码，在读取管理员密码后再与管理员卡中存储的密码进行认证，在确认之后应用程序才能继续运行并取得对读写机具的操作权。

为了便于软件的维护和扩展，采用了模块化设计的方式来实现其功能。而且由于各个终端功能不同，并非所有的模块都有必要使用，所以在安装时也可以将个模块独立安装，提高了系统的灵活性。模块结构如图 6.8 所示。

6.6　系统的扩展——多应用方案

随着 IC 卡技术的不断发展，越来越多的 IC 卡应用系统出现在和人们生活息息相关的领域。而在 IC 卡不断给人们的生活带来极大的便利的时候，却也带来了另外一个不便，那就是人们携带的 IC 卡片也越来越多。虽然相比之下，这点不便并不是很大的问题，但是仍然让人们在使用的时候觉得美中不足。因此，对于一张卡实现多种应用系统的要求逐渐被提到了日程之上。

对于一卡多用的解决方案，主要的思想就是在一张卡上划分好几张虚卡。所谓虚卡就是指屏蔽非该应用存储区的地址范围，使得从不同的应用系统的角度来看，是一张不同的卡片[24]。对于 CPU 卡，对存储区的划分可以由卡上的操作系统来管理，其大小和格式可以有很大的灵活性。而对于存储卡，由于没有卡上的 CPU，所以不能指望有卡内操作系统来管理，所以存储区在事先就需要划分为固定的大小，如 MF1 卡内的扇区，以便为不同的应用准备空间。但是这样会带来空间利用不合理的情况，灵活性也大打折扣。所以一般对于多应用系统多采用 CPU 卡来实现。

6.6.1 公交射频 IC 卡系统的扩展

公共交通领域包括有公共汽车、地铁、城市轻轨、出租车以及大型停车场等项目，在公共汽车公司引入了射频 IC 卡收费系统之后。可以考虑到在出租车、停车场等单位也引入电子收费系统。如上海就已经在公共汽车、地铁等场合采用一卡多用的收费系统。

在前面的公交电子收费系统中采用的是 MF1 型射频 IC 卡，虽然不是 CPU 卡，对于一卡多用的优势不明显，但是由于公共交通领域的应用项目大同小异，所以在公共交通领域内实现一卡多用还是足够的。

MIFARE®在设计 MF1 卡的时候就已经充分考虑了多应用实现的问题，并提出了 MIFARE®智能卡应用目录（MAD）[45]的概念已解决多应用的分配问题。在图 3.2 和 3.3 中详细描述了 MAD 的结构，MAD 存储在 MF1 卡的 0 扇区的 1、2 块中，用于存储不同应用系统的识别号和存储区地址指针。对于应用系统的识别号，MAD 要求在 MIFARE®处注册，目的在于大范围的多应用的协调适应性。而对于在城市公交系统内部的多应用实现。也可以设计自己的识别号格式，以便在应用系统的设计时更加灵活和有效的利用存储空间。

实际上对于 MF1 卡上多应用系统的设计，主要则是在对卡上 0 扇区文件记录的设计。在 0 扇区 0 块的存储区里，存储的是 MF1 卡的序列号，由于该块只能读不能写，所以这一块是不能作为多应用的目录区使用的。

而在 0 扇区中的其他三个块的访问由块 3 中的访问条件位来确定，也就是说，只有块 1 和块 2 在块 3 中的访问条件位的控制下才能作为存储多应用系统目录来使用。块 1 和块 2 总共有 32 个字节，而其余的存储器扇区只有 15 个，那么只要在这 32 个字节中能够存入 15 个扇区的应用设别号就可以了。

因为 MF1 卡的扇区是已经固定的地址范围，那么只需要将 32 个字节分成 2 个字节一个记录，那么以后面的 15 个纪录分别对应可用的 15 个扇区，在这些记录中存入应用识别号（2 个字节的长度足够公共交通领域的应用系统的数目了），对于空白的扇区使用 0000H 或者 FFFFH 来填充。这样，就可以为各个应用指定正确的存储扇区。

对于各个应用对其存取扇区的访问，则必须在白卡初始化的时候由应用系统向该扇区内写入应用系统自己的密钥后才能被该应用自由使用。以公共交通领域多应用为例，在公共汽车自动售票系统中使用了的 IC 卡占用了卡内的扇区 1~6，则其必须在扇区 1~6 的访问条件位中分别写入访问条件并以自己制定的密钥来替换密钥 A 和密钥 B。而如果新加入了出租车收费系统，那么，该系统就不可能再访问由公共汽车自动售票系统发售的射频 IC 卡的扇区 1~6 了，而是在公共汽车卡加入该系统的时候在卡中的扇区 0 的第 7~15 条记录中所要占用的扇区记录中写入该系统的应用标志号，然后再对相应扇区的块 3 进行操作。

由于 MAD 存储在 0 扇区，所以所有使用该 MAD 的应用系统都必须读取 0 扇区的内容以找到自己的存储区的位置，这就要求各个系统在 0 扇区的访问密钥必须统一。这样一来，对于该密钥就需要得到更加严密的管理，否则就有可能对多个系统同时构成威胁。

结 束 语

作为近年来逐渐兴起的智能识别的一种手段，IC 卡技术的应用越来越广泛。本文围绕着 IC 卡家族的新成员——射频 IC 卡的应用问题进行了深入的研究，并以公共交通系统中的应用为例描述了射频 IC 卡系统的实现情况。射频 IC 卡作为一种安全的数据载体，在系统中的应用主要体现在其安全系统和管理系统的设计上，亦即对卡上数据的流向管理问题。射频 IC 卡以其独有的特点，为其提供了方便的实现方案。另外，作为射频 IC 卡应用的趋势，多应用系统的实现问题在本文中也作出了设想。

由于射频 IC 卡的使用不受 IC 卡插槽的限制，在使用的时候有相当大的灵活性和方便性。而更重要的是在工作时间上有了很大的提高，所以在越来越多的领域开始应用。然而，由于其能量供给方式的限制，在卡上实现微处理器的嵌入一直是难以解决的问题，这导致射频 IC 卡在对安全性有非常高的金融系统和安全访问系统中的应用难以普及。所以，射频 IC 卡该如何发展，取决于对射频能量供给问题的解决。更低功耗要求的微处理器技术也是推动射频 IC 卡进一步发展的动力。本文的研究尚属肤浅，错误在所难免，讫望指正、帮助和指导。

致　谢

本文从一开始课题的选定，系统设计方案的确立，以及对具体现场的考察调研。一直到全文的撰写以及文稿的修改，都是在导师章兢教授的悉心指导下完成的。对其中设计思路的引导和论文的审校，更倾注了他大量的精力和心血。特别是在设计过程中，章教授经常能够一针见血的指出问题所在，让我从中得到很多的经验和启发。他广博的知识面，丰富的实践经验以及抓住问题要点的能力，使我受益匪浅，也将激励我在今后的工作和学习中丰富自己，努力进取。在此，特别向章兢教授表示由衷地感谢和诚挚的敬意。

另外，在课题的研究过程中得到了株洲建汉电子有限公司的各位工程师的帮助和指导。特别是在株洲调研期间得到了刘建汉工程师在生活和工作中给予的关心和帮助。在此，向刘工以及建汉公司的各位工程师表示感谢。

对所有在论文的撰写过程中给予关心和支持的老师、同学以及亲人致以深切的谢意！

刘　铮

二〇〇二年三月

参 考 文 献

[1] 边红丽．非接触 IC 卡技术及应用漫谈．世界产品与技术．2000．9．26~28

[2] [德] Klaus Finkenzeller． 射频识别（RFID）技术——无线电感应的应答器和非接触 IC 卡的原理与应用（第二版）． 北京：电子工业出版社． 2001

[3] 冯军．非接触式 IC 卡芯片的耦合电源及相关低压电路设计技术．电子质量．2001．3．18~19

[4] 冯晓君，李也白等．从 IC 卡的技术特性看其在综合性应用中的优势．计算机工程．2000．12．190~191，193

[5] 黄智伟．智能 IC 卡操作系统的功能分析．电子计算机与外部设备．2000．4．49~51

[6] 黄智伟，李富英．逻辑加密存储卡的操作控制程序设计．国外电子元器件．2000．4．40~42

[7] 季颖，范恒．非接触式 IC 卡电源产生电路原理与设计．微电子学．2000．2．127~129

[8] 景林．IC 卡数据组织和存取算法的研究及程序实现．计算机应用．2001．1．72~74

[9] 李池水，龚华志，杨贵才．射频卡数据读写方法．电测与仪表 2000.9．51~52.

[10] 李军，徐彤．数字密钥．中国电子商务．2000．15．29~29

[11] 刘嵩岩，毛志刚．智能卡的研究与发展．微处理机.2000．2．1~5

[12] 卢开澄．计算机密码学：通信中保密与安全． 北京：电子工业出版社．1992.9

[13] [美] B．施奈尔．应用密码学——协议 – 算法和 C 源程序．1995

[14] 潘晓雷，孙军等．密码技术在 IC 卡的应用模式．现代电子技术．2001．6．25~27

[15] 邱祖江，郭亚炜．一种改进 Miller 编解码的实现方法．微电子

学．2000．3．176~178
[16] 苏兵，徐松源．存储器 IC 卡数据传输的加密研究．哈尔滨理工大学学报．2000．4．63~65，69
[17] 涂航，刘玉珍．智能卡操作系统中 RSA 算法的实现与应用．武汉大学学报．自科版．2000．3．313~315
[18] 王爱英．智能卡技术——IC 卡（第二版）．北京：清华大学出版社．2000
[19] 王挺，吕述望．公钥密码在智能 IC 卡中的应用．微计算机应用．2000．4．199~202
[20] 王卓人，邓晋钧，刘宗祥．IC 卡的技术与应用．北京：电子工业出版社．1999
[21] 魏洁，付雪峰等．IC 卡的新时代－双界面．华南金融电脑．2001．6．65~65
[22] 吴欣，张华．MIFARE射频 IC卡及应用．管理信息系统．2000．7．58~61
[23] 夏熙梅，尚雅琴．射频识别技术及其应用．工业技术经济．2000．5．87~89
[24] 徐岩宇．城市公共交通“一卡通”系统．自动化博览．2000．5．36~38
[25] 俞林，甘骏人．一个适用于逻辑加密 IC 卡的认证加密方案．应用科学学报．2000．2．109~113
[26] 张飞舟，范跃祖，孙先仿．公交车辆非接触 IC 卡自动检票管理系统的开发与研究．自动化与仪器仪表 1999.3．35~36．
[27] 张吉文，郭圣文．IC 卡系统设计中的安全性考虑．微型机与应用．2000．2．17~18
[28] 张镕，陈彦章等．IC 卡系统安全措施浅析．江西电力职工大学学报．2000．4．26~29
[29] 赵学霖．公交 IC 卡收费系统．电子工程师．2000．2．22~23
[30] 庄旭晖，冯穗力．存储式 IC 卡的个人化及其数据读写程序设计．微型机与应用．2001．3．43~46
[31] 卓文．智能卡的操作系统：COS．电子与金系列工程信息．2001．4．20~25
[32] Asari Koji，Hirano Hiroshige．Ferroelectric memory circuit technology and the application to contactless IC card．IEICE Transactions on

Electronics. 1998 4. 488–495

[33] Couch II, Leon W. Digital and analog communication systems, Prentice – Hall Inc, London 1997

[34] Aleksander , Ken . Micromachined electro-mechanically tunable capacitors and their applications to RF IC's. IEEE Transactions on Microwave Theory and Techniques. 1998 12. 2587~2596

[35] Fummy, Walter, Cryptography, R. Oldenburg Verlag München Wien 1994

[36] Glogau, Ralf, Geheimsache, erschienen in: DOS, Heft 12/94, DMV Verlag

[37] Intergrated Silicom Design PTY LTD (ISD), Training Manual. Adelaide – Australia. 1996

[38] International Standard ISO/IEC , FCD 14443 . Identification Cards. Contactless Integrated Circuit(s) Cards – Proximity Cards
Part1: Physical Characteristics
Part2: Radio frequency power and signal interface
Part3: Initialization and anticollision
Part4: Transmission protocol

[39] Longo, G. Secure digital communications. Springer Verlag. New York 1993

[40] Mäusl, Rudolf, Digital Modulations, Hüthig Verlag, Heidelberg 1985

[41] Mansukhani. Arun. Wireless Digital Modulation, Applied Microwave &Wireless, Nov/Dec. 1996

[42] Ing. Fliege. Norbert, Digital Mobile system, B. G. Teubner, Stuttgart 1996

[43] Philips Semiconductors Gratkorn GmbH. Mifare System Overview 1998. www.semiconductors.philips.com

[44] Philips Semiconductors Gratkorn GmbH. Integrated Circuit, Mifare Standard Card IC MF1 IC S50 Functional Specification , May 2001. www.semiconductors.philips.com

[45] Philips Semiconductors Gratkorn GmbH. Standardization Note, Mifare Application Directory MAD, 1998. www.semiconductors.philips.com

[46] Philips Semiconductors Gratkorn GmbH. Reader Components, Mifare Serial Reader MFRD260, June 1997. www.semiconductors.philips.com

[47] Siebel. KW-Spezial-Frequenzliste. Siebel Verlag Wachtberg-Pech, 1983