
TTL UART/USB
超高频RFID读写模块设计手册
AS3992 读写芯片
(ISO18000-6C EPC G2)

基于 AS399x 的超高频 RFID 读写器设计

摘要:

RFID无线射频识别系统是一种非接触自动识别技术,其基本原理是利用射频信号的空间耦合的传输特性,实现对识别物体所带信息的自动化读取和识别。

RFID识别系统由三个部分组成:硬件部分、应用软件部分以及RFID数据格式的标准与通信协议。其中的硬件部份主要包括:RFID读写器(阅读器,Reader)、电子标签(应答器,Tag)以及天线。在使用中,RFID读写器循环扫描(轮询)读取电子标签数据,一旦标签进入读写器的天线有效范围内,读写器就可以读取RFID标签中的数据,从而完成对产品的信息收集。读写器可将数据通过通信接口传到主控制器或主机上,以作进一步的数据处理。

RFID系统的工作频率有多种,目前应用较为广泛的为125KHz、13.56MHz、920MHz。在商品应用领域使用较多的是EPC UHF G2标准,它是应用900MHz的UHF甚高频作为无线传输媒介。其相较于其它的标准,优点主要体现在传输距离远(可达10米以上)、标签价格更为便宜。随着国内经济的快速发展,相信EPC体系会有着广阔的前景。

AS399x读写器/读写模块不仅支持ISO18000-6C协议,还兼容18000-6A/B协议,可完成对符合这些协议的电子标签的所有操作,并提供完善的用户接口和用户端PC机或自主的控制器的操作函数,方便用户可靠、快速地完成对UHF电子标签的操作。用户可以应用读写器直接完成对电子标签的相关操作,如标签发行、标签识别等。也可以将读写模块嵌入到自己的产品中,使自身的产品具有电子标签识别的功能。

AS399X系列读写器/读写模块是我公司应用austriamicrosystems公司出产的AS399X芯片、silicon LABs的C8051F340芯片以及其它射频电路设计的。它具有集成度更高、性能更稳定、价格更合适等优点,可适用于识别EPC电子标签的多种应用场合。并可以嵌入到用户的产品中构成更多的应用。

第一章	绪论	1
第二章	RFID 技术工作原理及相关技术	3
2.1	RFID 系统的工作原理和技术	3
2.1.1	RFID 基本概念及特点	3
2.1.2	RFID 系统组成及工作原理	3
2.1.3	RFID 系统分类	4
2.1.3.1	按照频率范围划分	4
2.1.3.2	按照供电形式划分	5
2.1.3.3	按照调制方式划分	5
2.2	EPC Gen2 标准分析	6
2.2.1	EPC Gen2 协议的层次划分	6
2.2.1.1	物理层	6
2.2.1.2	标签识别层	6
2.2.2	通信信息传输	7
2.2.2.1	脉冲间隔编码	7
2.2.2.2	调制技术	8
2.2.2.3	FMO 码和 Miller 码	10
2.2.3	标签状态及状态间转移路径	11
2.2.4	标签盘存和访问步骤	13
2.2.5	Q 值计算方法	14
2.2.6	EPC Gen2 与 IS0180006A、6B 的比较	15
2.3	RFID 读写器设计分析	17
2.3.1	RFID 读写器的功能	17
2.3.2	RFID 读写器的组成结构	17
第三章	射频收发模块设计	19
3.1	射频收发模块技术指标	19
3.2	射频收发模块硬件设计	19
3.2.1	AS399x 射频收发芯片	20
3.2.1.1	芯片性能和特性	20
3.2.1.2	芯片结构	21
3.2.1.3	片上 PLL 和 VCO	23
3.2.1.4	射频发射部分	24
3.2.1.5	射频接收部分	26
3.2.1.6	工作模式及低功耗设计	26
3.2.1.7	AS399x 数据收发过程	27
3.2.2	C8051 单片机	30
3.2.2.1	性能和特点	30
3.2.2.2	芯片结构	31
3.2.2.3	CIP51 微控制器	32
3.2.2.4	FLASH 存储器和 ITAG 调试	33
3.2.2.5	可编程 IO 和交叉开关	34
3.2.2.6	其他通信端口	34

第四章 系统硬件电路设计	36
4.1 射频模块电路设计	36
4.1.1 差分输出电路及变压电路	36
4.1.2 低通滤波电路	37
4.1.3 压控振荡器及外围电路	38
4.1.4 定向耦合器电路	38
4.2 单片机电路设计	39
4.2.1 TTL UART 和 USB 接口电路	40
4.2.2 复位电路	40
4.2.3 JTAG 接口电路	41
第五章 系统软件设计	42
5.1 系统程序结构	42
5.2 系统程序设计与实现	43
5.2.1 总体流程	43
5.2.2 系统防冲突算法	43
5.2.3 写标签程序实现	45
5.2.4 读标签程序实现	47
5.2.5 锁标签程序实现	50
5.2.6 灭活标签程序实现	52
5.3 系统通信数据格式	53
5.3.1 系统命令	54
5.3.2 命令帧及数据帧结构	55

第一章 绪论

随着RFID技术的发展，RFID系统的结构和性能也会不断提高，越来越多的应用对RFID系统的读写器提出了更高的要求。RFID读写器的发展呈现了以下的趋势：

1. 多功能。为了适应市场对RFID系统多样性和多功能的要求，读写器将集成更多方便使用的功能，例如除了射频识别外，更集成红外识别功能、Zigbee组网通信功能等，移动式读写器不再是简单的终端，而且可以是通信网络中的路由。另外，为了适应某些应用，读写器将具有更多的智能性，具有一定的数据处理能力，可以按照一定的规则将应用系统处理程序下载到读写器中。
2. 小型化、便携化、嵌入式、模块化。随着RFID技术应用不断增多，人们对读写器使用是否方便提出了更高的要求，这就要求不断采用新的技术来减少读写器的体积，使读写器携带方便，使用方便，易于和其他的系统进行连接，从而使得接口模块化。
3. 成本更低。随着市场的普及以及技术的发展，读写器以及整个RFID系统的应用成本将会越来越低，最终实现所有需要识别和跟踪的物品都使用电子标签，未来读写器的价格将会大幅降低。
4. 多种数据接口。由于RFID技术应用的不断扩展和应用领域的增加，需要系统能够提供多种不同形式的接口，例如RS232、RS422 / RS485、USB、红外、以太网、蓝牙、无线网络接口以及其他各种自定义接口。
5. 多制式兼容。随着RFID技术的逐渐融合，以及市场竞争的需要，只要这些标签协议是公开的，或者是经过许可的，某些厂家的读写器将兼容多种不同制式的电子标签，以提高产品的应用适应能力和市场竞争能力。
6. 多频段兼容。为了使用不同国家不同地区的需要，读写器将朝着兼容多个频段、输出功率数字可调等方向发展。读写器可以支持多个频点，能自动识别不同频率的标签信息。而在多个频段的读写器中，目前又以超高频段读写器的研发为重点。与其他频段的RFID技术比较来说，超高频段的RFID技术具有识别距离远、

识别准确率高、识别速度快、抗干扰能力强、可穿透非金属材料等优点，所以成为RFID读写器技术的研究热点。

基于AS399x超高频射频芯片的读写器除了具有其他UHF频段EPC Gen2协议读写器的一般特点外，还具有特点：

1. 体积小。系统电路PCB板体积是90mmx49mmx0.51mm。AS3991射频芯片单芯片集成PA、VCO、PLL、电源管理器、DA / AD转换器等模块，使外置芯片减少，外围电路简单。同时，电容电阻大部分采用0603和0402封装实现，进一步减少读写器体积。
2. 多制式兼容。读写器同时支持EPC Gen2以及ISO 18000-6A/6B通信协议。可以兼容不同协议的电子标签。
3. 多频段兼容。读写器模块可工作在国标(920~925MHz)、美标(902~928MHz)、欧标(865~868MHz)等840MHz至960MHz工作频段。
4. 功耗低。主要表现在两方面：一是读写器可以在掉电模式、收发模式、监听模式三种模式之间切换。在不需要其工作的时候，可以最大限度降低芯片的功耗；二是在收发模式下(发射功率20dBm)，读写器功耗1.5~2W。相比目前主流的UHF射频芯片Intel R1000(发射功率18.5dBm时)，功耗高达2.5W。
5. 多接口。读写器预留RS232 / RS485接口、USB接口以及SPI接口，可以通过串口或者USB接口与上位机系统通信。

第二章 RFID技术工作原理及相关技术

本章详细阐述了RFID技术的基本原理、RFID系统概要及其各部分的组成。同时介绍了EPC Gen2协议的技术特点以及RFID读写器的设计分析。

2.1 RFID系统的工作原理和技术

2.1.1 RFID基本概念及特点

RFID技术是20世纪90年代兴起的一种非接触式自动识别技术，利用无线射频方式进行非接触式的识别和通信，实现对被识别物体的信息交互。基本方法是把RFID电子标签附在对象物体上，当物体接近固定式RFID读写器或者通过手持式RFID读写器则可以读出标签里的关于对象物体的相关信息，从而实现识别通信功能。RFID技术具有可靠性高、操作方便快捷、识别速度快、安全防冲突等优点，另外它克服了传统接触式识别技术操作不方便、识别距离近的缺点。目前它地被广泛应用于工业自动化、商品流通、物流管理等领域，而且其应用领域有不断扩展的趋势。

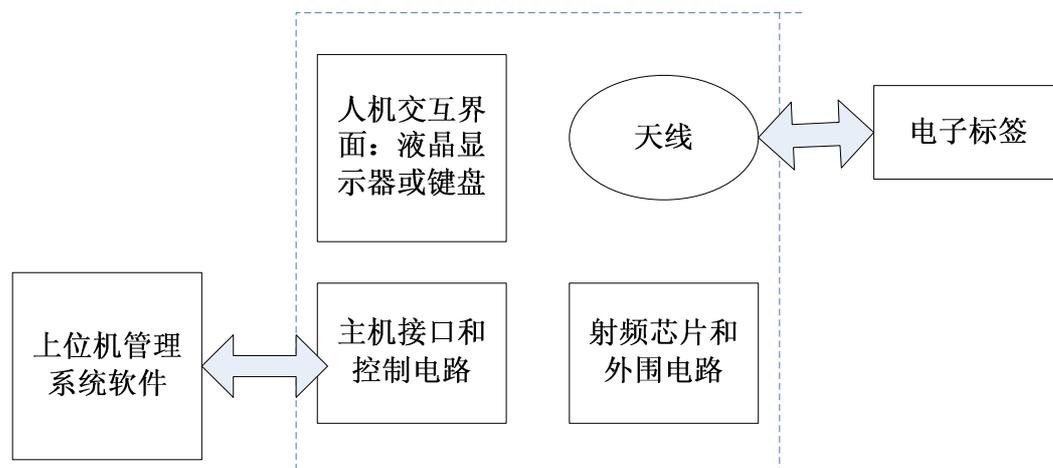
2.1.2 RFID系统组成及工作原理

一个RFID系统主要由四部分组成：

电子标签：由耦合元件及芯片组成，存储着必要的的数据信息。标签含有内置天线，用于和读写器射频天线间进行通信。

读写器：对存储于电子标签内的数据信息进行读写的设备。主要由射频电路、基带处理电路、电源模块以及必要的外围接口电路组成。

天线：在标签和读写器间传递射频信号。**相关应用软件：**根据不同的应用目的和场合，还有相应的上位机管理软件，对整个RFID系统的数据信息进行处理和存储。系统组成框图2.1所示。



电子标签为集成电路芯片。对于无源标签，工作时需要由读写器提供能量，读写器产生的射频载波用于为电子标签提供能量，一般通过整流方法将射频能量转化为直流电源存于标签的电容器中。而对于半无源电子标签来说，则通过该射频能量唤醒标签进入工作状态。有源电子标签一般自带电源模块，不需要利用读写器发出的射频能量。

读写器和电子标签之间的信息交互一般通常采用询问、应答的方式进行，即读写器发出询问信号后，电子标签予以应答。另一种情况是电子标签满足预先规定的工作条件后，主动发送信息，读写器根据电子标签发出的信息，进行存储或进一步发出询问请求，与电子标签构成一个完整通信过程，来达到读写器与电子标签之间进行数据交互的目的。无论那种情况，读写器和标签之间都必须有严格的时序关系，时序由读写器提供。

读写器和电子标签之间可以实现双向数据通信，电子标签存储的数据信息采用对载波的负载调制方式向读写器传送，读写器通过天线接收信息并上传给上位机管理系统进行信息处理，然后上位机把处理结果或者相关控制命令通过读写器和天线返回给电子标签。读写器给电子标签的命令和数据通常采用载波间隙、脉冲位置调制、编码调制等方法实现传送。

2. 1. 3 RFID系统分类

根据不同的分类标准，RFID系统可以有多种不同的分类。

2. 1. 3. 1 按照频率范围划分

RFID系统的工作频率可以划分为下述频段：

1. 低频(LF, 频率范围是30~300kHz)：工作频率低于135kHz, 最常用的是125kHz。主要协议有ISO11784、ISO14223。
2. 高频(HF, 频率范围是3~30MHz)：工作频率为13.56MHz。主要协议有ISO15693、ISO14443、ISO18000-3。
3. 超高频(UHF, 频率范围是300MHz~3GHz)：工作频率是433MHz, 866~960MHz以及2.45GHz。主要协议有ISO18000系列和EPC Gen2。
4. 甚高频(SHF, 频率范围是3~30GHz)：工作频率是5.8GHz和24GHz, 但是目前24GHz基本没有采用。

门禁和安全管理系统的应用是低频RFID系统的主要应用之一, 公交IC是高频RFID系统的主要应用之一, 物流供应链上的管理和应用则更多使用到超高频RFID系统。而随着物联网以及泛在网络概念的提出, 超高频RFID更是成为目前的研究热点。

2. 1. 3. 2 按照供电形式划分

根据标签供电的形式不同, RFID系统可分:

1. 有源系统: 电子标签使用内置电池来供电, 有源系统的识别距离相比较下较长。由于不需要担心功耗的问题, 有源系统可以实现的功能也比较多。缺点是受限于内置的电池, 使用周期比较短并且成本相对比较高。
2. 无源系统: 电子标签没有内置电池, 主要通过读写器发射的电磁场能量来唤醒标签的芯片工作。由于无需内置电池, 且靠外部唤醒, 所以这系统特点是体积小、寿命长、成本低, 但是实现的功能简单。
3. 半有源系统: 标签带有内置电池, 但只是起到激活系统的作用。电子标签首先被内置电池激活, 激活后的前部操作就无需电池供电, 即可进入无源电子标签工作模式。

2. 1. 3. 3 按照调制方式划分

根据调制方式不同, RFID系统可以分为:

1. 主动式系统: 读写器利用射频能量主动发送数据信息给电子标签, 调制方式可以是调幅、调频或者调相三者中的一种。

2. 被动式系统：系统使用反向散射调制的方式发送数据，标签必须利用读写器发出的没有经过调制的连续载波来承载自己的有用信号。

3. 半主动式系统：电子标签内部的电池的作用只是对电子标签内部电路供电，电子标签并不通过自身的能量主动发送数据给读写器，而是在标签通过读写器射频信号被激活后，通过反向散射调制方式传送自身的有用数据。

2. 2 EPC Gen2标准分析

2005年1月EPC Gen2申请成为ISO / IEC 18000-6C，2006年6月15日EPC C1G2正式进入ISO / IEC18000-6标准系列，它对ISO / IEC18000-6A和ISO / IEC18000-6B两种协议特点进行了一系列有效的修正与扩充。其中物理层数据编码、调制方式、防碰撞算法等一些关键技术都有了改进，使得ISO / IEC18000-6C的性能相比A、B有了很大的提高。本文读写器设计是基于EPC Gen2标准的，工作频率是860MHz-960MHz。下面简要介绍ISO / IEC18000-6C(EPC Gen2)标准特点及与A、B之间的比较。

2. 2. 1 EPC Gen2协议的层次划分

2. 2. 1. 1 物理层

物理层规定读写器与标签通信的**物理介质、通信速率、编码方式、调制方式等**。在EPC Gen2协议当中，读写器向标签发送的信息采用脉冲间隔编码(PIE)格式的双旁带振幅移位键(DSB-ASK)、单边带振幅移位键控(SSB-ASK)或反向振幅移位键控(PR-ASK)调制射频载波信号。标签通过相同的调制射频载波接收功率。读写器通过发送未调制射频载波和倾听反向散射回答接收从标签发来的信息。标签通过反向散射调制射频载波的振幅或相位，传达信息。用于对读写器命令作出响应的编码格式或是FMO或是Miller调制的副载波。具体编码格式参看2.2.2.1到2.2.2.3小节。

2. 2. 1. 2 标签识别层

EPC Gen2规定读写器利用三个基本操作管理标签群：

1. 选择(Select)：选择标签群以供盘存和访问。可连续使用Select命令根据

用户标准选择特定的标签群。

2. 盘存(Inventory): 即标签识别。读写器发出Query命令, 开始一个盘存周期。一个或一个以上的标签可以做出回答。读写器探测某个标签做出的回答, 请求标签发出的PC、EPC和CRC-16。盘存指令集除了Query命令外, 还包括: QueryAdjust命令, 用于调整Q值大小; QueryRep命令, 用于指示标签使其槽计数器减值, 若槽计数器在减值后槽等于0, 则应向读写器反向散射一个RN16; ACK命令用于确认标签以及NAK命令用于使标签返回仲裁状态。

3. 访问(Access): 即与标签通信, 读取标签发出的信息或将信息发送给标签。访问前必须要对标签进行唯一确定。访问命令集包括: Req_RN命令, 用于指示标签反向散射一个RN16; Read、Write、Access、BlockWrite以及BlockErase命令用于标签数据读写或擦除操作; Lock命令用于锁定标签, 使其数据不被读出或者写入; Kill命令用于灭活标签。

2. 2. 2 通信信息传输

通信信息的传输包括读写器到标签以及标签到读写器两个通信方向。

2. 2. 2. 1 脉冲间隔编码

读写器向电子标签传输的数据编码采用脉冲间隔编码(Pulse Interval Encoding, PIE)。在PIE编码中, 通过定义脉冲下降沿之间的不同时间宽度来表示4种符号(0, 1, SOF, EOF)。Taft时间段称为基本时间段, 它为符号0的相邻两个脉冲之间的时间宽度, 基准值为 $20\mu\text{s} \pm 100\text{ppm}$ (ppm表示基准值为 10^{-6})。符号0, 1, SOF, EOF编码的波形如图2. 2所示, 编码方法如表2. 1所示。编码时, 字节的高位优先编码。

表 2-1 PIE 编码方法

符号	编码持续时间
0	Tari
1	2Tari
SOF	Tari 后跟 3Tari
EOF	4Tari

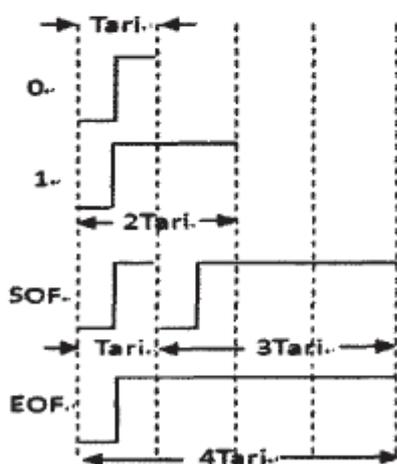
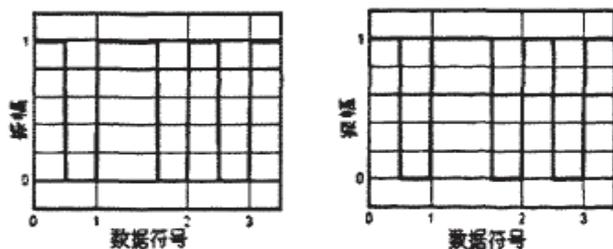


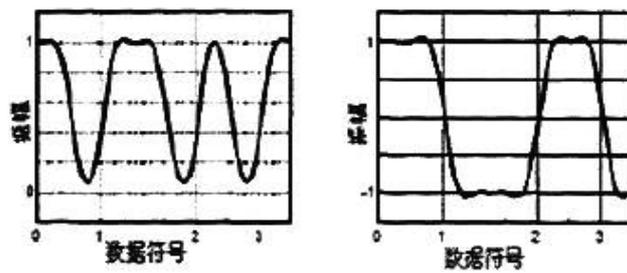
图 2-2 PIE 编码波形

2. 2. 2. 2 调制技术

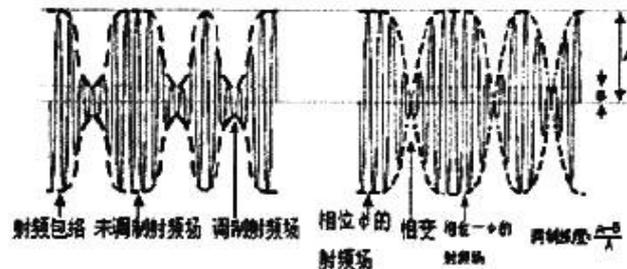
在发送时，读写器支持如下3种调制方式：双边带幅度调制(DSB-ASK)，单边带幅度调制(SSB-ASK)以及相位反转幅度调制(PR-ASK)。而标签应该可以解调所有这3种调制信号。具体的基带、调制及解调后的波形见图2. 3。



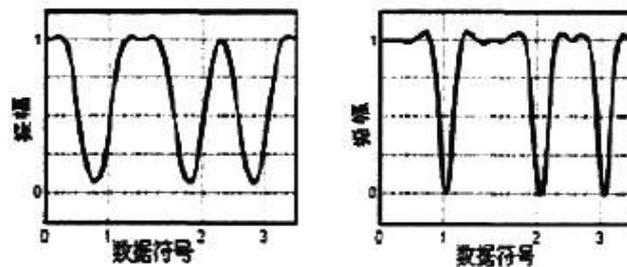
A. DSB-ASK 或 SSB-ASK (左) 和 PR-ASK 基带数据



B. DSB-ASK 或 SSB-ASK (左) 和 PR-ASK 调制波形



C. DSB-ASK 或 SSB-ASK (左) 和 PR-ASK 调制射频



D. DSB-ASK 或 SSB-ASK (左) 和 PR-ASK 检测波形

图 2-3 读写器对标签调制

DSB-ASK是载波信号开关键控(OOK)最容易生成的调制，但其频带宽度是调制信号带宽的两倍，由于上下两个边带是完全对称的，它们都携带了调制信号的全部信息，仅传输其中一个边带即可，所以说,DSB-ASK是带宽效率最低。改善带宽效率的方法之一是使用SSB-ASK。SSB-ASK调制方式在传输信号时只传输一个边带，不但节省了载波发射功率，而且它占用的频带宽度是DSB-ASK的一半，因此大大提高了频带利用率。

另外一种调制是PR-ASK。它可以使窄带中的载波噪声比要求达到最小，使到终端的功率传输达到最大。与相移键控(PSK)信号类似，PR-ASK每次发送符号时改变相位180。PR-ASK还可以采用100%的幅度调制深度，旧符号和新符号的相位矢量交叉，并简单地加总成零幅度。在幅度简单地变成零时，这提供了可

以简便检测到的时钟信号，同时使载波功率关闭的时间达到最小，从而优化传输到无源终端的功率。PR-ASK拥有载波噪声比和带宽要求，与DSB-ASK相比，其更加紧密地匹配PSK，使其对窄带远程应用极具吸引力。

2. 2. 2. 3 FMO码和Miller码

标签向读写器返回的数据采用FMO码或者Miller码编码。

图2. 4显示了生成FMO编码的基本功能和状态图。FMO在每个边界倒转基带相位，数据0有一个附加的中间符号相位倒转。图2-4的状态图描绘了所发送的FMO基本功能的逻辑数据序列。S1. S4状态标记表明四种可能FM编码符号，代表各FMO基本功能的两个相位。状态转换图映射发射逻辑数据序列时，FMO编码间的转换方向。例如，从状态S2转换到状态S3是不允许的，因为由此产生的传输在符号边界上没有相转化。图2-5显示了所发生的基带FMO符号和序列，应始终在每次传输结束时以dummy数据1结尾。

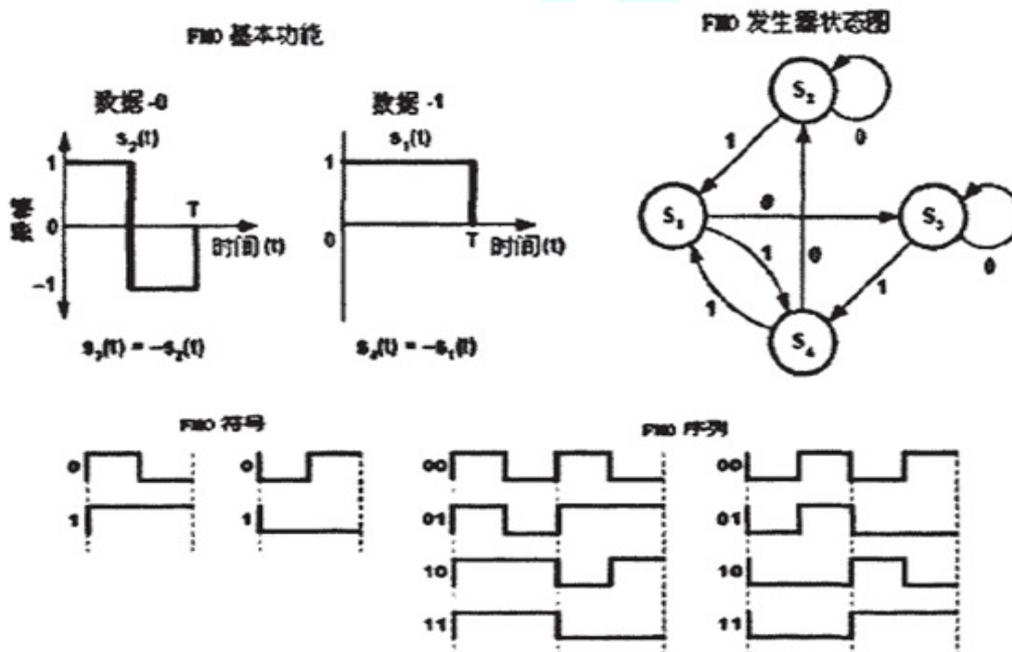


图2-6显示了生成Miller编码的基本功能和状态图。Miller码是双相码的一种变形。编码规则是：“1”码用码元间隔中心出现跃变来表示，即用“10”或者“01”表示。“0”码有两种情况：单个“0”时，在码元间隔内不出现电平跃变，而且与相邻码字边界也不跃变，连“0”时，在两个“0”码的边界处出现跃变，

即“00”与“11”交替。图2-6所示的状态图描绘了基带Miller基本功能的逻辑数据序列。S1、S4状态标记表明四种可能Miller编码符号，其符号组合(01 / 10 / 11)不发生相位翻转。图2-7显示了Miller调制副载波序列，Miller序列每位应包含2、4或8个副载波周期，具体情况由启动该盘存周期的Query命令规定的M值而定。Miller编码应始终在每次传输结束时以dummy数据1结尾。

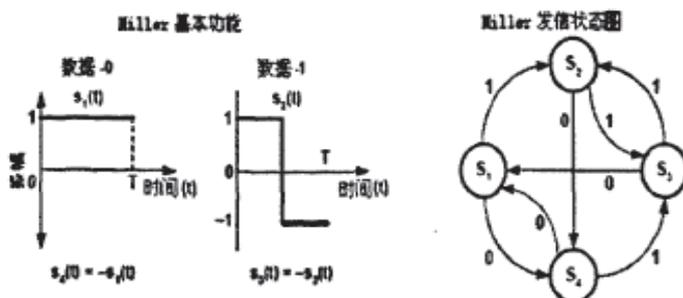


图 2-6 Miller 编码的基本功能和状态图

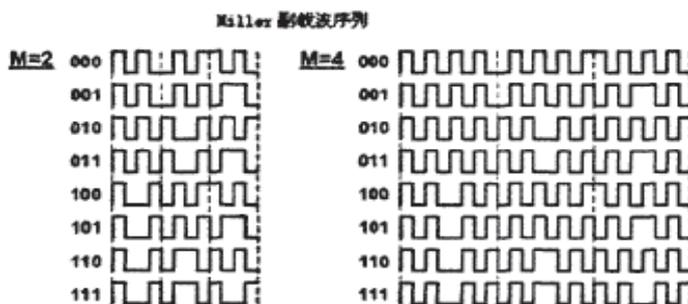


图 2-7 Miller 调制副载波序列

2. 2. 3 标签状态及状态间转移路径

读写器对标签的基本操作以及标签状态如图2. 8所示：

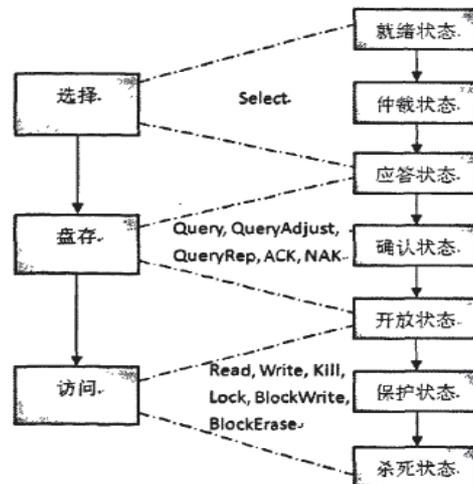


图 2-8 读写器对标签的基本操作以及标签状态

根据EPC Gen2通信协议，读写器在对标签群进行操作的时候，标签主要在以下几种状态之间切换：

1. 就绪状态

通电标签被灭活后或者正参与当前某盘存周期的保持状态。进入射频场后，没有被灭活的标签则进入就绪状态。标签保持它的就绪状态直至收到已盘参数和sel参数和自己匹配的Query命令。匹配的标签从0到20_1中随机抽取一个随机数载入其槽计数器内，如果该随机数为零则转换到应答状态，进行下一步操作；否则，转换到仲裁状态。

2. 仲裁状态

参与当前盘存周期但槽计数器数值不等于零的标签的保持状态。处于仲裁状态的标签在每次收到通话参数与当前盘存周期通话匹配的QueryRep命令后使它的槽计数器减1，直到槽计数器减到0时，转换到应答状态；否则，继续接收QueryRep命令并减槽计数器数值，直到其为0为止。

3. 应答状态

槽计数器数值为零的标签进入应答状态，反向散射RN16。之后若标签收到含有相同RN16的ACK确认命令，则转换到确认状态，反向散射其PC、EPC和CRC-16；如果标签未能接收到ACK或收到无效ACK（即所含RN16有误），则应返回仲裁状态。

4. 确认状态

处于确认状态的标签根据收到的具体命令，可以转换到除灭活状态之外的任何状态。

5. 开放状态

处于确认状态且访问1:3令非零的标签在收到Req_RN命令后转换到开放状态，同时反向散射新的RN16，新的RN16作为句柄需要在随后读写器对标签的一系列访问操作中进行验证。处于开放状态的标签可以执行除Lock命令之外的所有访问命令，可以转换到除确认状态之外的任何状态。

6. 保护状态

处于确认状态且访问VI令为零的标签收到Req_RN命令后应转换成保护状态，反向散射新的RN16。处于开放状态且访问口令非零的标签在收到有效Access命令即转换到保护状态，保持原来的句柄不变。处于保护状态的标签可以执行所有访问命令，可以转换到除开放或确认状态之外的所有状态。

7. 灭活状态

处于开放状态或保护状态的标签在收到Kill命令后以有效非零灭活口令进入灭活状态。进入灭活状态后，标签不再对读写器的命令做出任何响应。

2. 2. 4 标签盘存和访问步骤

读写器发出Select命令选择特定的标签群后，读写器从中唯一确定一张标签并对该标签进行访问操作。具体流程如图2-9所示：读写器首先发一个含有Q值的Query命令。参与标签在收到Query命令后，在 $(0, 2Q - 1)$ 范围内挑选一个随机数值载入槽计数器。随机数等于零的标签换成应答状态并立即作出应答。随机数非零的标签不作出反应，继续等待读写器发出的QueryAdjust或QueryRep命令；当标签进入应答状态后即反向散射RN16，读写器以含有相同RN16的ACK命令确认该标签；之后，被确认的标签转换到确认状态，反向散射其PC、EPC和CRC-16；读写器发送含有与之前相同的RN16的Req_RN命令，标签反向散射一个新RN16作为应答；最后，读写器以新的RN16作为访问句柄，对标签进行访问操作。

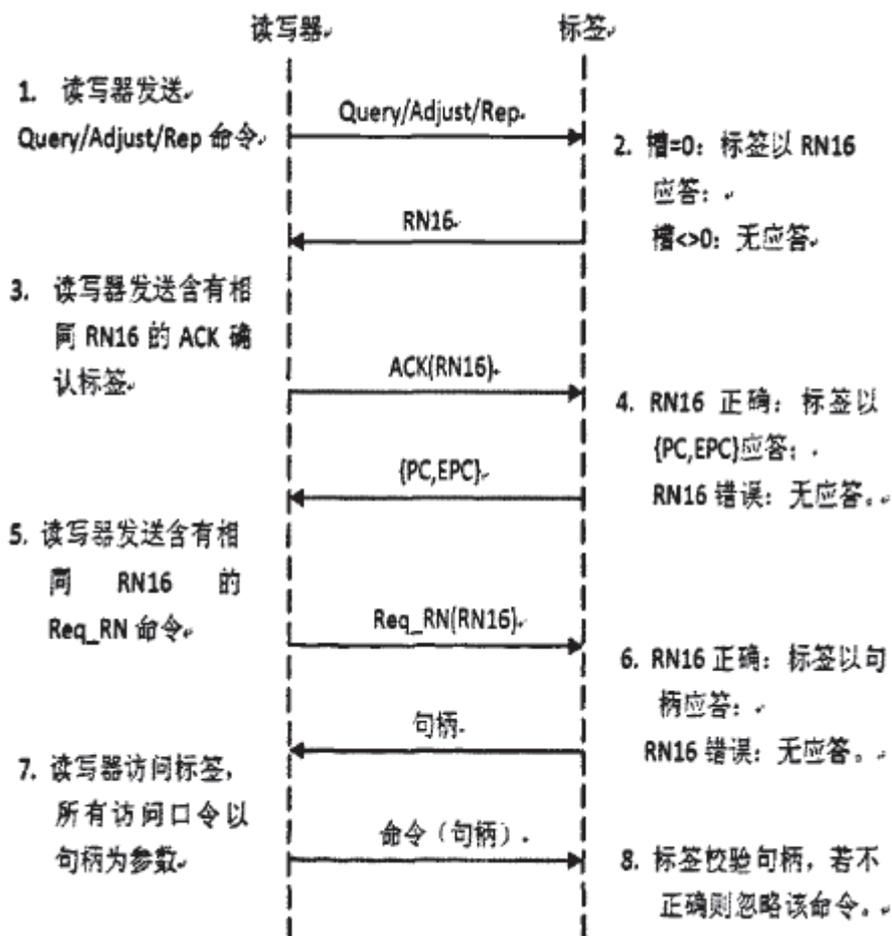


图2-9 标签盘存和访问步骤

2. 2. 5 Q值计算方法

EPC Gen2标准中推荐了一种调整Q参数的方法，如图2-10所示：

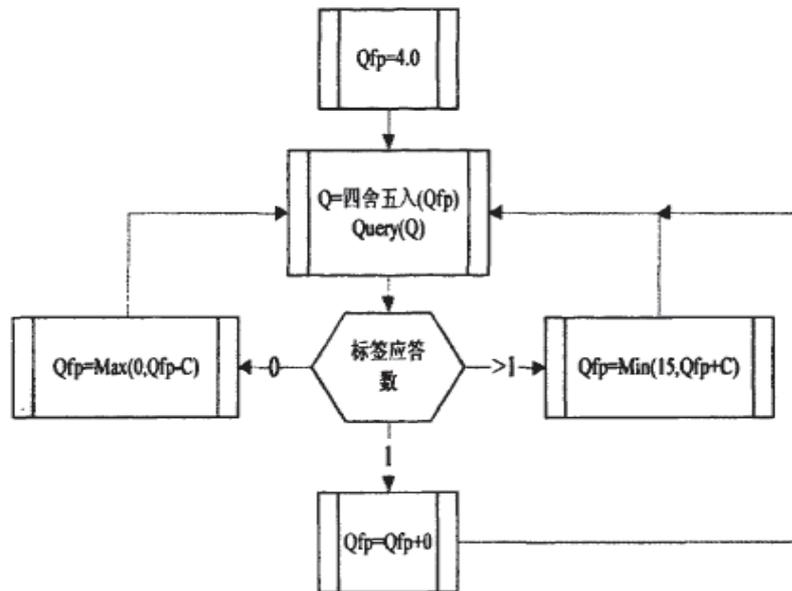


图2-10 参数Q选择算法

1. 开始一轮发送循环时，将浮点数Q币初始化成4.0。
2. 将Qfp取整，得到Q，即 $Q = \text{round}(Qfp)$ 。
3. 发送Query命令。
4. 查应答的标签个数n，调整Qfp的值：如果n等于0，即没有标签应答，则减少Qfp，即 $Qfp = \max(0, Qfp - C)$ ，其中C是在(0.1, 0.5)范围内的一个浮点数。在Qfp较大时，C取较小值；而Qfp较小时，C取较大值；如果n大于1，说明多个标签应答，或者说检测到冲突时，增大Qfp，即 $Qfp = \min(15, Qfp + C)$ ；如果n等于1，即只有1个标签应答，Qfp不变。
5. 回到第2步，直到完成一轮发现循环。

采用EPC Gen2标准中的算法优势一是系统的总体识别时间较少，系统吞吐率高；二是阅读器中初始帧长值(即Q值)的设置不受限制。劣势是系统由于调整帧长过于频繁而造成功耗的增加。

2. 2. 6 EPC Gen2与ISO180006A、6B的比较

ISO / IEC 18000-6C仅对EPC Gen2标准中标签存储器部分的内容和功能做了一些修改，其他部分继承了EPC Gen2标准的全部内容。与ISO / IEC 18000-6A、6B以及此前的EPC Gen1相比，ISO / IEC 18000-6C(EPC Gen2)具有以下的特点：

1. 高速率。在美国达到1500标签 / 秒，在欧洲达到600标签 / 秒。
2. 加密技术更加完善。数据的安全性能得到提高，同时提供了更大的内存读写空间，更好地满足各种应用的需求。
3. 功能更加丰富。可以在高密度(多个识读者)环境下工作，标签在芯片内集成了防冲突机制，保证被多个读写器读取时读取率的完整，有效提高了数据读取的准确性和可靠性。
4. 允许用户对同一标签进行多次的读写，支持长达256位的唯一物品识别码UII。相对比之下，EPC Gen1只支持最多96位的电子产品编码，ISO / IEC 18000-6A和ISO / IEC 18000-6B的唯一识别码UID均只是64比特。

ISO / IEC 18000-6C(EPC Gen2)标准相比于其他标准，在频段选择、物理层数据编码调制技术、标签访问控制、防冲突技术和数据加密等关键技术方面都有了很大的改进，这使得它在性能上比第一代EPC RFID标准有了显著的提高。

表2. 2对ISO / IEC18000-6标准的三种类型作了简单比较。

表2.2 ISO / IEC 18000-6 A / B / C协议比较

		6A	6B	6C
读写器到 标签	工作频段	860~960MHz	860~960MHz	860~960MHz
	速率	33kb/s	10kb/s 或 40Kb/s	26.7~128kb/s
	调制方式	ASK	ASK	DSB-ASK
				SSB-ASK 或 PR-ASK
编码方式	PIE	Manchester	PIE	
标签到读 写器	副载波频率	未用	未用	40~640kHz
	速率	40kb/s	40kb/s	FM0: 4~640kb/s
				子载频调制:
				5~320kb/s
	调制方式	ASK	ASK	ASK 或 PSK
编码方式	FM0	FM0	FM0 或者 Miller 调制子	

				载频
	唯一识别符长度	64 比特	64 比特	最小 16 比特，最大 496 比特
防碰撞	算法	ALOHA	Adaptive binary tree	时隙随机反碰撞
	类型(概率或确定型)	概率	概率	概率

2.3 RFID读写器设计分析

2.3.1 RFID读写器的功能

读写器可将主机的读写命令传送到电子标签，再把从主机发往电子标签的数据加密，电子标签返回的数据经过解密后送到主机。主机的数据交换以及管理系统主要完成数据信息的存储和管理、对电子标签进行读写控制等。具体说来，读写器应该具备以下的功能：

1. 以射频方式为无源或半有源电子标签传输能量；
2. 在射频区域内查询多个标签，并能正确区分各个标签，可以与电子标签进行数据交换；
3. 可以对固定对象和移动对象进行识别；
4. 可以提示读写过程中发生了错误，并显示错误的相关信息；
5. 读写器可以通过标准接口如USB、RS232等与主机网络连接。提供下列信息以实现多个读写器在系统网络中的运行：本读写器的识别码、本读写器读出电子标签信息的日期和时间、本读写器读出的电子标签的信息。

2.3.2 RFID读写器的组成结构

读写器电路组成框图如图2.11所示。各部分的作用简述如下。

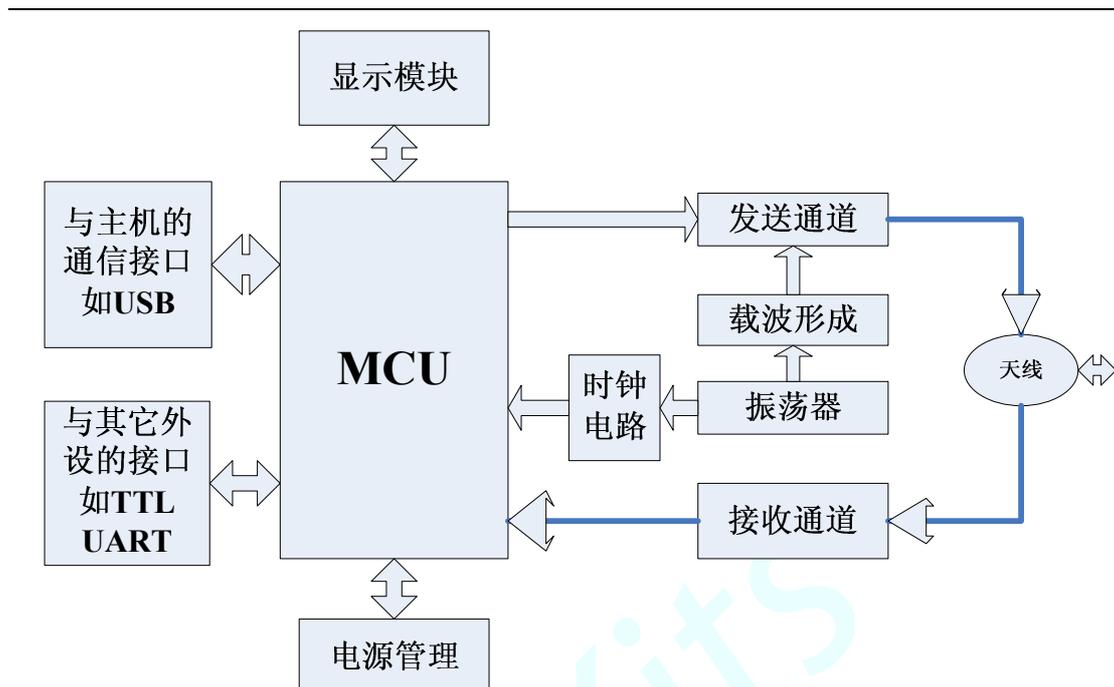


图2-11 RFID读写器电路组成

振荡器：振荡器电路产生符合RFID系统要求的射频振荡频率，一路经过时钟电路产生MCU所需要的时钟信号，另外一路经过载波形成电路产生读写器工作的载波信号。

发送通道：发送通道包括编码、调制和功率放大电路，用于向电子标签传送命令和写数据。

接收通道：接收通道包括解调、解码电路，用于接收电子标签返回的应答信息和数据。同时还应该考虑防碰撞电路的设计。

微控制器(MCU)：MCU是读写器工作的核心，完成收发控制、向标签发送命令和写数据、标签数据读取和处理、与应用系统的高层进行通信等任务。

电源管理器：通过读射频读写部分的独立电源控制，系统可以在MCU中根据需要选择开启或者关闭射频读写功能。当应用系统有低功耗要求，不需要射频模块芯片一直工作的时候，这种控制方式是必不可少的。

天线：天线的作用就是产生磁通量，为无源标签提供电源，在读写设备和标签之间传送信息。天线的有效电磁场范围就是系统的工作区域。

第三章 射频收发模块设计

射频收发部分是读写器很重要的部分，负责接收上位机系统发送到主控芯片的命令，读写器根据命令对数据信息进行编码和调制，发送到电子标签中以实现数据通信。同时，读写器接收来自电子标签的信号并进行解调和解码，再根据上位机的命令对接收的数据进行处理。

3.1 射频收发模块技术指标

根据所采用的国际标准EPC Gen2和实际的应用条件，所设计的基于AS399x的射频收发模块技术指标如下表3.1所示：

表3.1 射频收发模块技术指标

通信协议	EPC Gen2/ISO 18000-6A/B/C
工作频率	840~960MHz
功耗	1.5W~2W
调制方式	ASK 或 PR-ASK
编码方式	FM0 或者 Miller
射频功率	最大 20dBm
数据传输速率	40kbps
读写距离	1~6m
工作模式	命令(或者触发)
通信接口	TTL UART 或者 USB
天线接口标准	MMCX
电源	+5.5V DC
物理尺寸	90mm×49mm×0.51mm

3.2 射频收发模块硬件设计

射频收发模块分为射频电路部分以及单片机电路部分。射频芯片采用奥地利

微电子公司的AS399x射频芯片，MCU采用C8051F340单片机。

3. 2. 1 AS399x射频收发芯片

3. 2. 1. 1 芯片性能和特性

AS399x是奥地利微电子公司推出的单片射频收发器芯片，工作于915MHz频段，同时支持ISO 18000-6C(EPC Gen2)以及ISO 18000-6A/B通信协议。工作电压是5.3伏。采用64引脚QFN封装(9mm×9mm)。

AS399x是一款高集成度的射频芯片。在发射电路端，集成了功率放大器(PA)、锁相环(PLL)、压控振荡器(VCO)、频率合成器、调制器等模块；在接收电路端集成了低噪声放大器(LNA)、混频器(Mixer)、中频放大器、解调器等模块。同时还集成了电源电压管理、协议控制等工作模块，从而使芯片外围电路大大简化。芯片控制通过32个寄存器的设置来实现全部RF、滤波及协议控制功能。收发模块支持自动生成帧头和CRC校验码，组装成帧的数据块通过片上的24字节FIFO寄存器传输到上位机系统中。电源管理模块可以对片外MCU以及其他芯片供1.5~3.3伏电压以及提供时钟输出。片上PA具有高达20dBm的输出功率，片上VCO和PLL可产生840MHz-960MHz的振荡频率。

综上所述，AS399x射频芯片具有一下特性：

1. 支持多通信协议；
2. 高集成度，外围电路简单；
3. 低工作电流；
4. 输出功率可达20dBm；
5. 可选择时钟输出提供给MCU；
6. 支持和MCU之间的8位并行或者4线串行通信；
7. 采用ASK或者PR-ASK信号调制；
8. 可选择接收增益控制；
9. 支持三种工作模式间切换，大大降低功耗。

AS3991的基本参数如下表3.2所示：

表3.2 AS3991的基本参数

参数	数值	单位
供电电压	5.5	V
监听模式输出电流	3	mA
休眠模式输出电流	20	uA
收发模式输出电流	150	mA
内置 PA 功率	20	dBm
待机模式工作频率	63	KHz
正常工作模式频率	10	MHz
温度范围	-55~+125	摄氏度

3. 2. 1. 2 芯片结构

AS3991射频芯片的结构框图如图3.1所示：

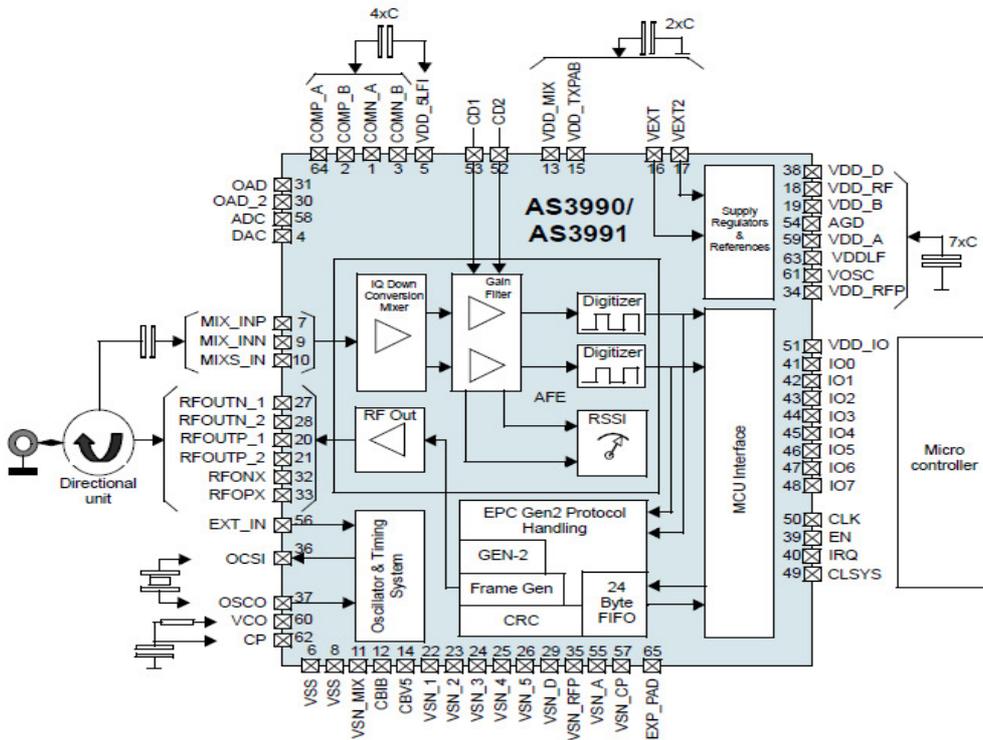


图3.1 AS3991的结构框图

AS3992射频芯片的结构框图如图3.2所示：

3. 2. 1. 3 片上PLL和VCO

AS399x片上集成PLL，由压控振荡器VCO、分频器、鉴相器和电荷泵组成。如图3-2所示，环路中的÷N分频器可采用可编程分频器，合成器的输出频率为：

$$f_0 = Nf_r \quad (3.1)$$

式3.1中， f_0 为环路鉴相器PD的输入鉴相频率，也称之为参考频率。 f_r 是从高稳定的晶体振荡频率，即基准频率 f_1 ，经参考分频器分频(÷R)取得的。这种合成器的频率分辨率即为参考频率 f_r 。

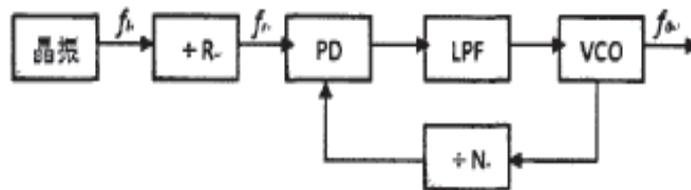


图3-2 频率合成器电路

外围电路需要搭建环路滤波器把CP引脚端的输出信号进行滤波，环路滤波器很大程度上决定PLL的动态性能。VCO的振荡信号被馈送到分频器和功率放大器，输入电压范围是0~3.3V，产生的频率是860MHz~960MHz。AS399x也可以配合外置VCO工作，如图3-3所示。寄存器PLL auxiliary中的位B22、B21以及B20决定使用内置还是外置VCO。

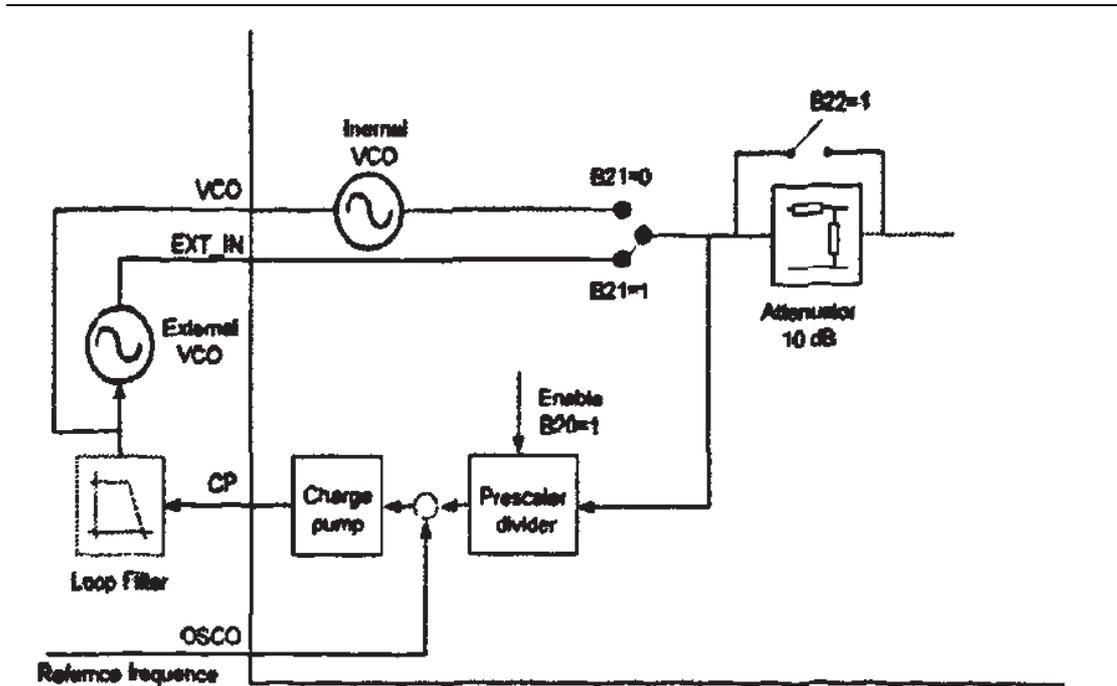


图3-3 系统与VCO的接法

3. 2. 1. 4 射频发射部分

MCU输出的符号数据先后经过基带编码、调制滤波和信号放大。AS3991射频芯片支持片内编码调制、片外编码片内调制以及片外编码调制三种方式。本设计采用片内编码调制方式,无需外置调制解调电路。信号调制采用ASK信号调制。原理框图如图3-4所示,通过模拟相乘的方法实现ASK调制。

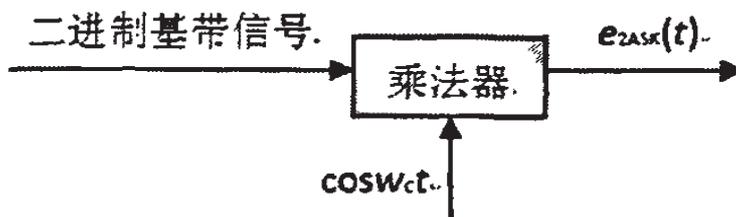


图3-4 二进制ASK信号调制器原理图

信号调制后,需要经过PA进行信号放大。AS3991有两种PA输出模式,如下图3-5所示。通过设置Regulator and IO control寄存器进行模式选择。

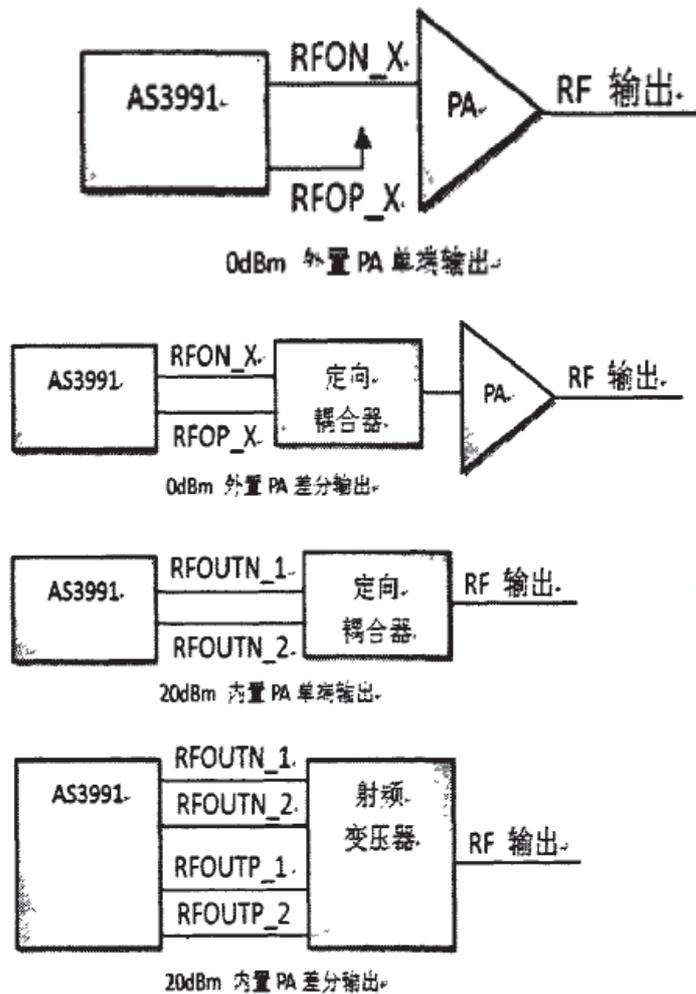


图3-5 系统与PA的接法

1. 低功率输出 (0dBm): 这模式需要使用外置PA把输出信号进行放大, 同时外围电路需要加上外部射频扼流圈和去耦合电容进行滤波。引脚有两种连接方式, 分别是单端输出和差分输出: 前者把AS3991的RFON_X引脚和外置PA连上, RFOP_X引脚接地; 后者分别把RFON_X和RFOP_X与外置PA连上。我们的读写模块采用了这种接法。

2. 高功率输出 (20dBm): 这模式使用片上集成PA, 适用于长距离应用场合。使系统正确运行需要外部射频扼流圈和正确的操作匹配阻抗。高功率输出同样有单端输出和差分输出, 前者分别把AS3991的RFOUTN_1和RFOUTN_2引脚和外围定向耦合电路连上; 后者则把RFOUTN_1、RFOUTN_2、RFOUTP_1和RFOUTP_2分别和外围定向耦合电路连上。

3. 2. 1. 5 射频接收部分

AS3991/AS3992射频芯片集成的接收电路实质上是I/Q两路结构的零中频接收机。电路结构如图3-6所示。接收信号被分成I和Q两路信号，本振信号通过移相形成相差90°的两路信号，分别进入两个混频器进行下变频，混频器的输出经过滤波去除本振和高次谐波后，得到的低频信号就是标签返回的信息。

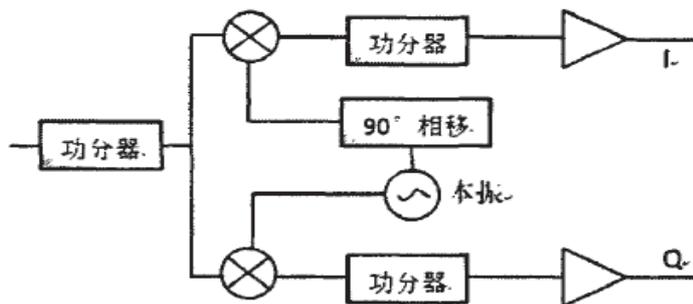


图3-6 零中频正交混频检波电路

本振信号分为两路，两者相位相差90度，如下式：

在通道I中：

$$V_{oI}(t) = A_{L0} \times \cos(\omega t + \varphi_{L0}) \quad (3.2)$$

在通道Q中：

$$V_{oQ}(t) = A_{L0} \times \cos(\omega t + \varphi_{L0} + \pi/2) = A_{L0} \times \sin(\omega t + \varphi_{L0}) \quad (3.3)$$

通道Q的本振信号与接收信号混频后经滤波可得：

$$\begin{aligned} V_s(t) &= A_c \times [1+m(t)] \cos(\omega t + \varphi_c) \times A_{L0} \sin(\omega t + \varphi_{L0}) \\ &= 1/2 \{ A_c A_{L0} [1+m(t)] [\sin(2\omega t + \varphi_c + \varphi_{L0}) + \sin(\varphi_c - \varphi_{L0})] \} \\ &\approx 1/2 \{ A_c A_{L0} [1+m(t)] \sin(\varphi_c - \varphi_{L0}) \} \end{aligned} \quad (3.4)$$

从式3.4看出，I路中和本振相乘后，是COS函数，而Q路中是sin函数，所以I/Q两路的零点交替的。当其中一路输出为零时，另一路的输出最大，而且两路的输出之和始终为一个恒定的常数，I/Q两路结构的零中频接收机克服了传统零中频接收机的零点效应。

3. 2. 1. 6 工作模式及低功耗设计

AS3991/AS3992有三种工作模式：

1. 休眠模式。可以通过软件设置EN引脚电平,当EN=L,即低电平时,AS399x进入休眠模式。

2. 收发模式。AS399x在正常工作时候处于收发模式,此时EN=H。在此模式时,电源调节器、VCO、PLL、晶体振荡器等模块都正常工作。晶体振荡器频率CLSYS最后稳定在10MHz(可调),芯片处于随时可以收发数据的状态。

3. 监听模式。可以通过软件设置位stby=H,之后AS399x从收发模式进入到待机模式。在待机模式中,VCO和晶体振荡器工作在低功耗模式,CLSYS频率是60kHz;PLL、数据收发等工作模块休眠停止工作。

本设计充分利用AS399x三种工作模式的特点,从而把功耗降到最低。EN信号控制CLSYS频率在63kHz和10MHz之间的跳变,Chip Status Control寄存器中的stby位控制系统在监听模式以及收发模式之间的切换,两个信号由软件控制。当系统上电后,EN=L, sbty=H,此时CLSYS频率等于63kHz,系统首先进入休眠模式,等待上位机发送的控制命令。直到收到控制命令,读写器置位EN=H, Sbty=H不变,系统进入监听模式,大部分模块仍然停止工作或者工作在低功耗模式下,电流为3mA,此时系统不断监听是否有标签进入到射频场内。如果有,系统设置sbty=L,所有工作模块上电工作,进入收发模式读写射频场内的标签,此时电流是150mA。当读写完成后,系统把sbty软件置位同时把EN软件复位,系统重新进入休眠模式等待上位机指令。系统从以上步骤实现模式的切换,而在收发模式时,读写器功耗仅是1.5—2W,远低于目前主流的UHF射频芯片Intel R1000的2.5W。此方式适用于手持式读写器设计。

如果使用于固定式读写器,系统可以在监听模式和收发模式间直接切换,而无需切换到掉电模式等待指令。

3. 2. 1. 7 AS399x数据收发过程

AS399x数据发送过程是:

MCU启动数据发送同时装载要发送的数据到FIFO寄存器。数据长度被写入TX length寄存器,数据则被装载进FIFO寄存器。当装载入控制命令以及数据长度和相应的数据后,传输就开始了。

如果待发送的数据长度长于FIFO的长度，MCU会先填写满24字节长度的FIFO寄存器并开始发送数据，之后当FIFO只剩下3字节待发送数据时，AS399x发送一个中断请求。MCU通过读取IRQ status register查看中断原因。之后根据FIFO剩余长度空间再装载待发送的数据进去，如此循环，直到全部数据发送完毕。当发送操作完毕后，AS399x通过IRQ status register产生另外一个中断通知MCU发送完毕。数据发送流程图如图3-7所示：

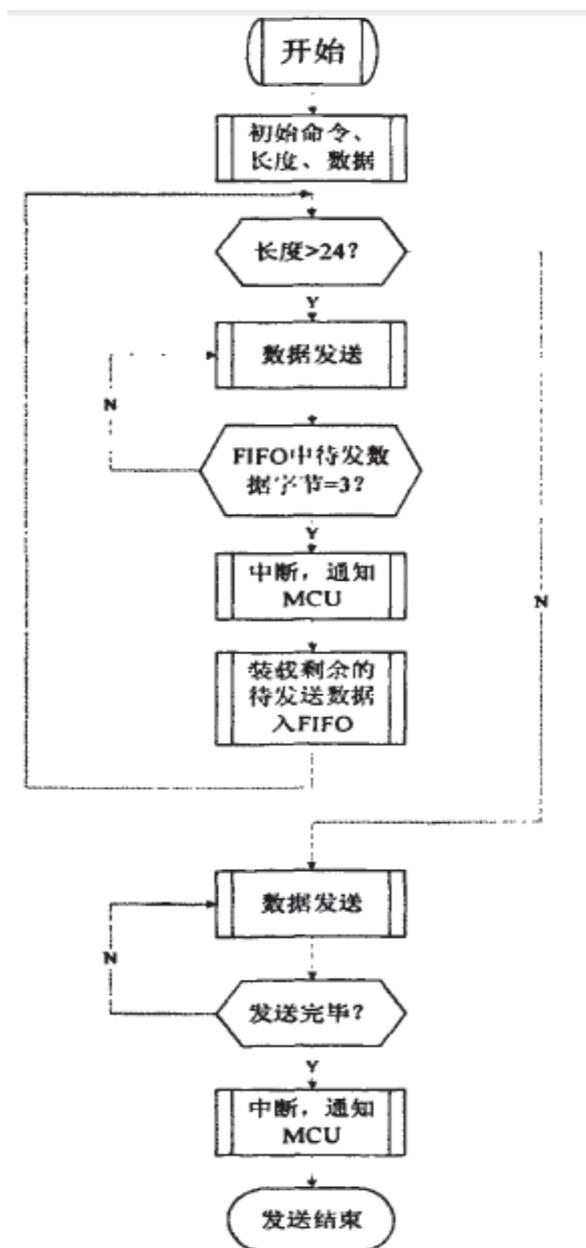


图3-7 AS399x数据发送流程

AS399x数据接收过程：

接收模块采用零中频接收机形式，通过90度相差形成IQ两路正交解调器电路。接收到的射频信号经过滤波器和低噪声放大器放大后，与互为正交的两路本振信号混频，分别产生同相和正交两路信号。由于本振信号频率和射频信号频率相同，所有混频后直接产生基带信号。

在模拟信号解调后，进行数据解码。首先是对各种协议位解码，即根据Protocol control寄存器和RX options寄存器的设置信息，把子载波编码信号转换成比特流和数据的时钟。第二步是根据通信协议检查并去除数据帧头和CRC校验位。之后数据被送到24字节长度的FIFO寄存器中被MCU读取。

数据接收可是和结束都通过IRQ and status寄存器产生中断标志通知MCU。如果所接收的数据长度大于8个字节，当接收第9个字节的时候则产生一个中断标志，通知MCU把之前接收到的在FIFO中的数据清空，预留空间给继续接收的数据。同样地，如果接收数据的数据格式或者CRC校验码错误，AS399x也产生中断通知MCU。数据接收流程图如图3. 8所示：

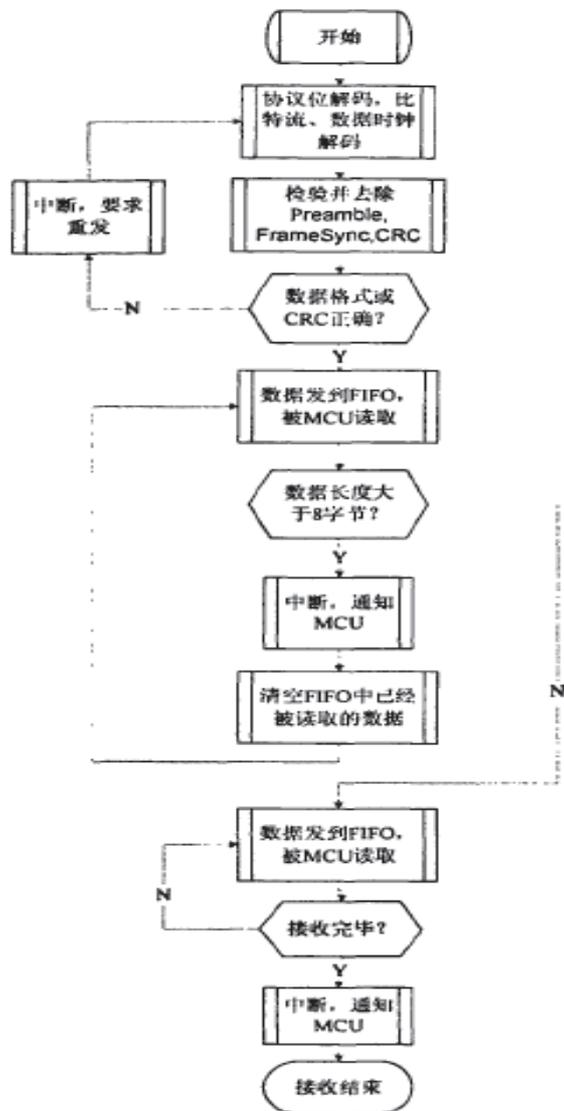


图3-8 AS399x数据接收流程图

3. 2. 2 C8051单片机

3. 2. 2. 1 性能和特点

本设计采用的是Silicon Labs公司推出的C8051F系列单片机。C8051F系列单片机是SoC的典型代表，单芯片集成度十分高，片上集成丰富的模拟和数字资源。具有与8051兼容的高速CIP-51内核，单片机处理速度和性能都有很大的提升，而且开发简单，容易移植，成本也十分低，是目前应用最广泛的单片机种类。C8051F340芯片的特点总结如下：

- 1、与8051兼容的CIP-51微控制器内核，有效提高程序执行速度。

- 2、集成在系统调试接口，方便开发与二次开发。
- 3、丰富的模拟资源，提高系统的可靠性。
- 4、丰富的外部设备接口，不仅降低了系统成本，更降低了系统功耗。
- 5、增强了在信号处理方面的性能。
- 6、独立的片内时钟源，有利于系统整体功耗的降低。
- 7、提供空闲模式及停机模式等多种电源管理方式来降低系统功耗。
- 8、实现了I/O从固定方式到交叉开关配置。
- 9、复位方式多样化，为保障系统的安全、操作的灵活性以及零功耗系统设计带来极大的好处。

3. 2. 2. 2 芯片结构

C8051F340的结构框图如下图3-9：

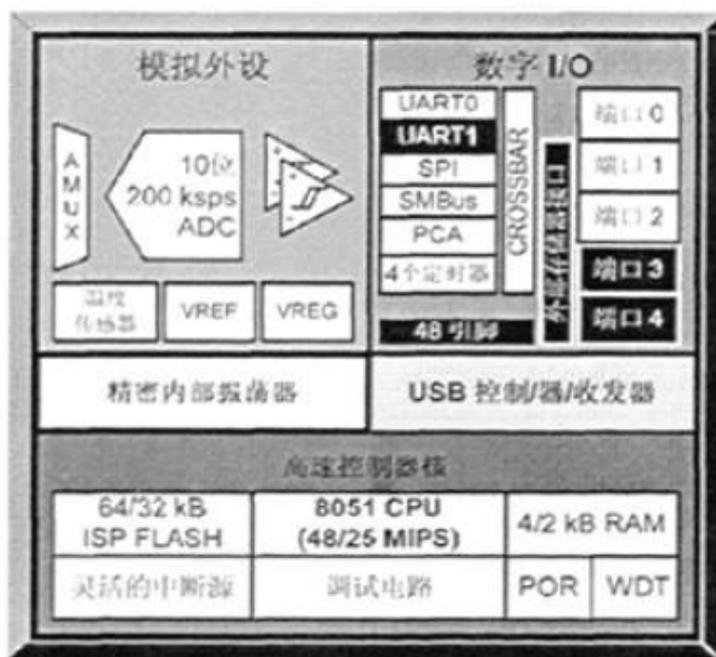


图3-9 C8051F340的结构框图

C8051F340MCU单片集成了大量的模拟和数字资源。模拟资源有ADC子系统、数/模转换器、模拟比较器等；数字资源包括三个16位定时器/计数器、256 byte内部RAM、UART、片内可编程计数器/定时器阵列以及SPI总线和SMBus/12C总线。有多达7个复位源：片内VDD监视器、看门狗定时器、时钟丢失检测器、

件，包括计数器/定时器、内部RAM、UART、特殊功能寄存器等。此外还包含片内调试硬件，在一个集成电路内提供了完整的数据采集以及控制系统解决方案。

在吞吐量方面：C1P-51采用了流水线结构，即每个时钟脉冲都接受下一条数据指令，各数据指令同时执行，所以它的指令吞吐量要远超过标准8051系列。在后者中，绝大部分指令都需要12或24个系统时钟周期，最大系统时钟频率12MHz。

对于CIP-51内核，70%的指令只需要1个或两个系统时钟周期，只有4条指令需要执行超过4个系统时钟周期，没有超过8个系统时钟周期的指令。CIP-51的最大时钟为25MHz，相对应的最大处理能力为25MIPS。除此之外，CIP-51内核还增加了定制外设和功能，大大增强了它的处理能力。

3. 2. 2. 4 FLASH存储器和ITAG调试

C8051F340单芯片内部集成可在系统和在应用编程的FLASH存储器，用于非易失性数据存储以及程序代码存储，并可以通过程序软件对FLASH编程。本设计系统通过Silicon Labs 2线(C2)接口对FLASH存储器进行编程。C2接口采用两条数据线在宿主机和器件之间传输数据：时钟信号线和双向数据信号线。本系统和程序下载器U-EC5之间的线路连接如图3-11所示：

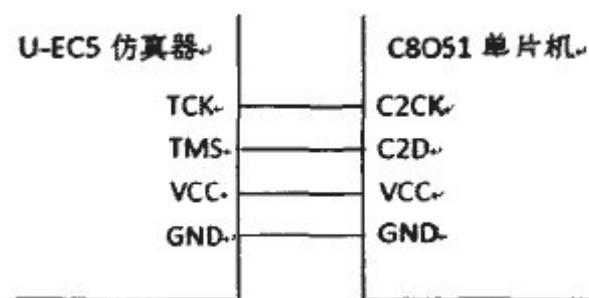


图3-11 系统和U. EC5的连接

其中，U. EC5的TCK是时钟线，TMS是双向数据线。

Silicon Labs调试系统有一系列的特性，如：支持观察和修改寄存器和存储器、支持断点、观察点等一系列功能。这些特性使进行系统调试时不需要外部资源的支持，并且与此同时，系统的模拟和数字外设都可以如常工作不受到影响，

从而使得系统效率更高。

3.2.2.5 可编程IO和交叉开关

C8051F340有40个I/O引脚。端口引脚组织如图3-9所示。每个端口引脚都可以被定义为通用I/O(GPIO)或模拟输入, P0.0~P3.7可以被分配给内部数字资源。本设计系统的I/O分配是: P0.4和P0.5分别是串口数据输入输出引脚, P0.3是外部中断输入, P0.7是系统时钟输入, P1.0~P1.7是8位数据传输, 其他I/O并未使用。这种资源分配的灵活性是通过使用优先权交叉开关译码器实现的。

C8051F340引入数字交叉开关, 改变了以往内部功能和芯片引脚固定的对应关系。它允许将内部数字系统资源灵活地分配给P0、P1和P2端口。见下图3-12。这种结构可支持所有的功能组合, 可以通过设置交叉开关控制寄存器, 把片内的SMBus、SPI、UART、PCA、计数器/定时器、串行总线、硬件中断、以及微控制器内部的其它数字信号等配置为出现在端口I/O引脚。从而不同用户可以根据自己特定的应用场合或需求, 通过软件编程选择通用端口I/O和所需数字资源的组合, 更加灵活地实现资源分配。

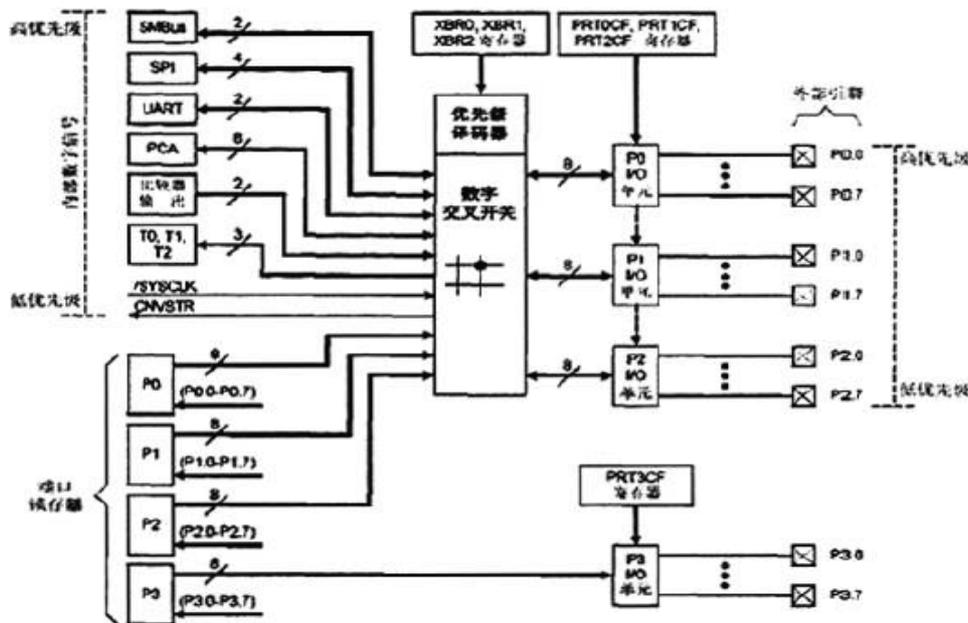


图3-12 C8051F340端口引脚组织

3.2.2.6 其他通信端口

CS051F340MCU内部集成丰富的通信端口，包括了：一个完整的USB功能控制器、两个异步全双工UART、一个增强型SPI总线和一個SMBus / 12C总线。

USB功能控制器用于实现USB外部设备，由串行接口引擎、USB收发器、IKB FIFO存储器以及时钟电路组成。不需要另外再搭建外部元器件便直接可用；两个异步全双工UART分别是UART0和UART1，两者都通过相关的特殊功能寄存器来具体工作模式进行设置；增强型串行外设接口提供了访问全双工同步串行总线的能力。工作时既可以作为主器件又可以是从器件，可以使用3线或4线方式，而且可以在同一总线上支持多个主器件和从器件：SMBus I/O接口是一个双线的双向串行总线，与12C串行总线兼容。

Eleckits

第四章 系统硬件电路设计

AS399x单芯片内部集成了数模 / 模数转换、调制解调等工作模块，以及集成了PA、PLL和VCO，只需在芯片外部使用电阻电容搭建一环路滤波电路，整个压控振荡电路即可正常工作；射频信号经过内置PA放大之后，差分输出20dBm信号。信号经过变压器、滤波器和定向耦合器后，由射频天线发射出去。同时，C8051单片机集成电源管理模块、USB管理模块、SPI以及UART串行接口。由于AS3991以及08051芯片的高集成度，使得系统所需要的芯片以及外围电路得到减少和简化，从而有效降低系统成本。系统的各芯片选型如表4.1所示。

表4.1 系统芯片和选型

芯片	选型
射频芯片	AS3991/AS3992
单片机芯片	C8051F340
低通滤波器	LFCN 1000
平衡变压器	Balun_D900BL
PA 芯片	SPA-2118

4.1 射频模块电路设计

系统射频模块主要功能是产生高频发射能量、激活电子标签并为电子标签提供能量；对发射信号进行调制，把数据传输给电子标签；接收并解调来自电子标签的射频信号。射频模块负责对射频信号的处理和数据的传输，完成对电子标签的读写操作。

本系统射频模块设计主要包括射频输出及定向耦合器电路、环路滤波电路、压控振荡器及外围电路以及晶振电路。

4.1.1 差分输出电路及变压电路

系统射频输出采用内置0dBm差分输出。示意图如图4-2所示。

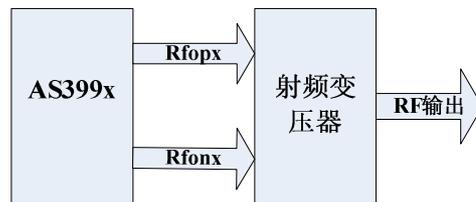


图4-2 射频差分输出

信号通过 AS399x 射频芯片引脚端 Rfopx、Rfonx 差分输出。信号输出通过 LC 匹配网络,以改善驻波比,提高输出功率及改善非线性特性。平衡变压器 Balun 用于把双端差分输出转变为单端输出。巴伦是平衡-不平衡变换器(Balanced to Unbalanced) 的音译,用于将功率相等相位相反的平衡信号转换为单端不平衡信号,送至不平衡负载;反之,亦可将不平衡信号转换为平衡信号。此外,它还能提供阻抗变换功能,所以又叫做平衡馈电器。正是由于这些特点,使得巴伦在微波技术与天线领域得到了广泛的应用。

4. 1. 2 低通滤波电路

在射频信号进入定向耦合器输出前,射频信号先经过低通滤波器滤除不需要的信号成分和高频噪声。系统低通滤波器采用LFCN 1000,截止频率是1300MHz,通带最大驻波比(VSWR)是1.3,插入损耗0.8dB。

LFCN 1000是一款LC低通滤波器。原理图如图4-3所示,通过串联多个电感同时并联多个电容形成。其中电容具有“阻直流,通交流”的作用,而电感则有“通直流,阻交流,通低频,阻高频”的作用。当伴有许多干扰噪声的信号通过LC滤波电路时,交流干扰信号大部分将被电感阻止吸收变成磁感和热能,剩下的大部分被电容旁路到地,从而起到有效抑制干扰信号的作用,在输出端获得比较纯净的有用信号。



图4-3 LFCN 1000原理图

当系统差分输出信号经过Balun变为单端输出后,信号通过LFCN 1000进行

低通滤波，分离出有用信号。

4. 1. 3 压控振荡器及外围电路

系统采用内置VCO，所以只需要在外围电路搭建一个环路滤波器即可。如图4-4所示。

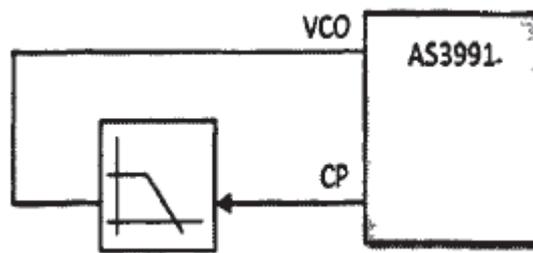


图4-4 外置VCO示意图

环路滤波器是低通滤波器。它是由电阻、电容等组成的线性电路。它的作用是滤除电荷泵输出的高频分量和噪声，取出直流分量去控制VCO的输出频率。环路滤波器实现了改善控制电路的频谱纯度的功能。本设计在二阶无源滤波器中再加入一个RC低通滤波级，从而形成三阶无源滤波器，这种结构可以减少参考杂散和抑制环路的噪声。环路滤波电路如图4-5所示：

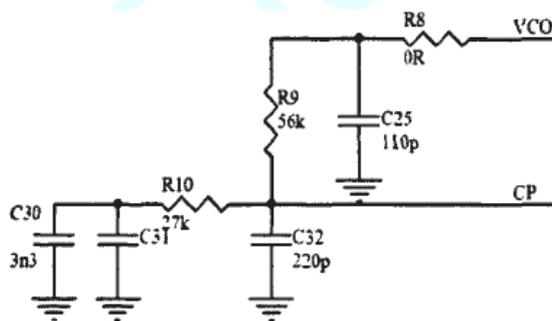


图4-5 环路滤波电路

4. 1. 4 定向耦合器电路

定向耦合器是四端口器件：输入端、连通端、耦合端以及隔离端。耦合端与连通端不同的是：耦合端与输入端是电隔离的（容性或者感性）。理想情况下，无论输入电压有多大，隔离端输出为零。如果给隔离端加电压，输入端输出也是零，即输入端与隔离端互相对称隔离。定向耦合器与发射机接收机的连接方式如下图

4-6所示:

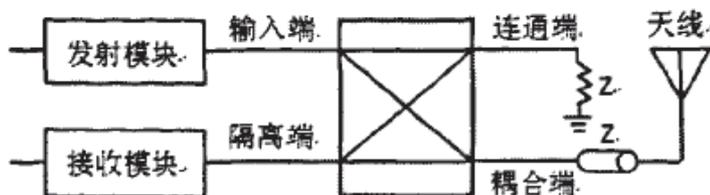


图4-6 定向耦合器示意图

发射机信号不会泄漏到隔离端，而是经过天线发射出去，即接收机不会接收到发射机发送的信号，由天线接收的信号则直接进入接收机。本系统采用RCP890A05定向耦合器，带宽是815~960MHz，耦合度5dB，插入损耗是-0.19dB，方向性小于等于-21dB。

4.2 单片机电路设计

单片机电路的主要功能是与应用系统软件进行通信；执行从应用系统软件发来的动作命令；控制射频模块与标签的通信过程；基带信号的编码和解码；执行防冲突算法；对读写器和标签之间传输的数据进行加密和解密；进行读写器和标签之间的身份认证等等。

单片机电路包括晶振电路、USB和UART接口电路、复位电路以及JTAG接口电路。如图4-7所示。

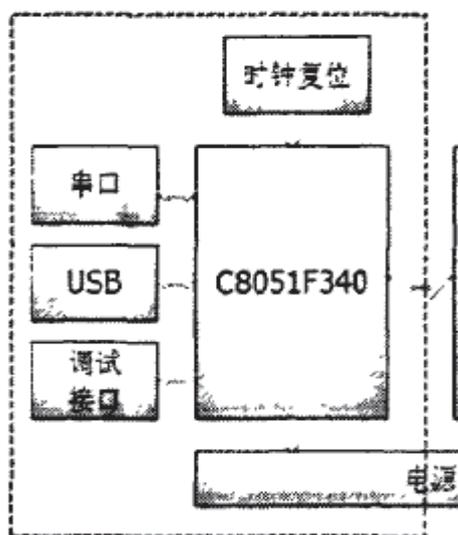


图4-7 单片机电路框图

4. 2. 1 TTL UART和USB接口电路

本系统与计算机的通信采用USB接口，并且引出TTL UART接口和与AS399x相连的MCU I/O口，电源3.3V、5V、GND。

通常情况下，嵌入式系统的TTL/CMOS电平与PC机的RS-232接口的逻辑电平不兼容，TTL电平的标准逻辑“1”一般对应2V~3.3V电平，逻辑“0”对应0V~0.4V电平，而RS-232标准采用负逻辑方式，逻辑“1”对应-3V~-15V电平，逻辑“0”对应+3V~+15V电平，因此，两者间的通信必须经过电平转换电路进行电平转换。我们可以用一个TTL转RS232模块或者TTL转USB模块连接到PC。

本系统可以通过USB接口和上位机之间进行通信。因为C8051F340单片机芯片本来已经集成USB管理模块，所以不需要外围的匹配电路和下拉电阻。USB接口电路原理图如下图4-8所示：

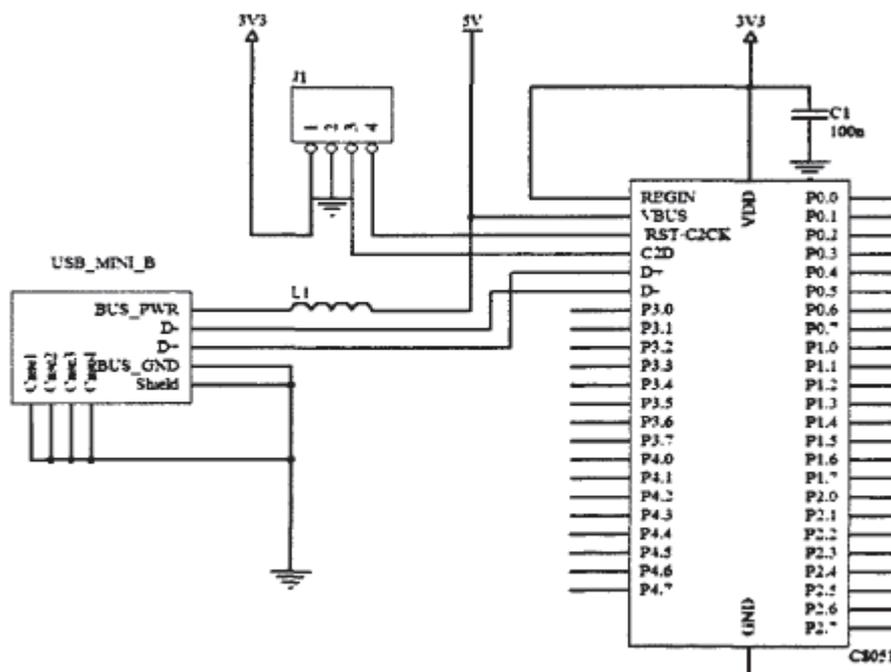


图4-8 USB模块电路图

4. 2. 2 复位电路

通常复位电路有三种情况：上电复位、手动复位和软件复位。

本系统中，复位电路通过两个去耦电容、一个上拉电阻和一个按钮实现手动复位。同时，系统也可以实现软件复位，电阻R4连接P4.7和reset引脚，程序只

需要把 P4.7 置零，即可实现软件复位。复位电路如图 4-9 所示

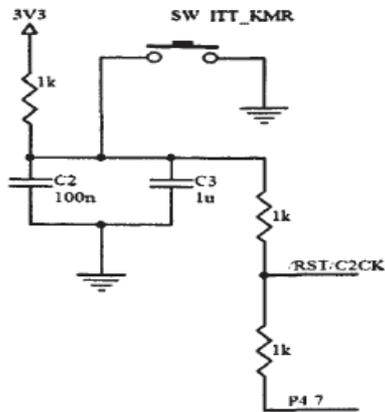


图4-9 复位电路图

4. 2. 3 JTAG接口电路

JTAG(联合测试小组)是一种国际标准测试协议，主要用于芯片内部测试及对系统进行仿真和测试。在本系统中，JTAG接口用于FLASH烧录程序和仿真接口。JTAG接口主要是4条信号线：TMS、TCK、TDI、TDO，分别为测试模式选择、测试时钟输入、测试数据输入和测试数据输出。

本系统中，JTAG的TMS和单片机C2D(双向数据端口)连接，TCK和单片机的C2CK(时钟信号)连接，TDI和TDO悬空，另外再接上3.3V电源和地线。

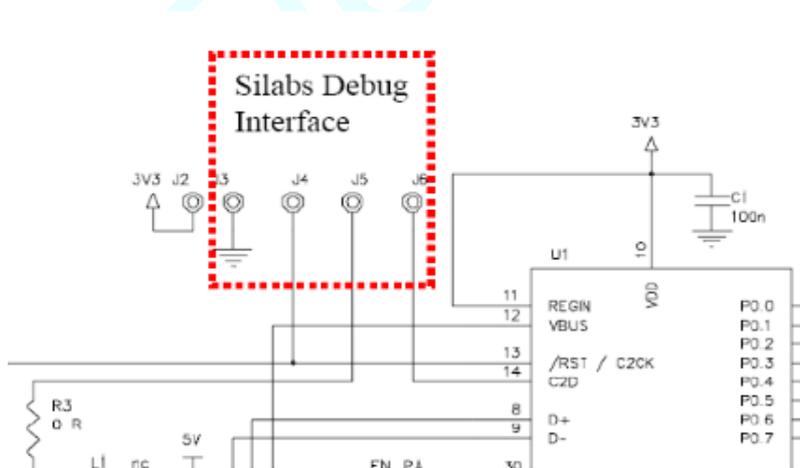


图4-10 C2

通过此C2口烧写固件时需要一个烧写器，最好再配上我们的JTAG转C2的转接板，然后可以直插在读写模块C2引脚接口，方便烧写。



注：也可以通过USB接口烧写程序，但要先通过C2口将引导程序烧写进去。这样USB就可烧写固件了。

第五章 系统软件设计

5.1 系统程序结构

射频识别系统是一种实时系统。在软件结构上，可以分成两部分：主程序和中断程序。主程序的主要任务是不断进行系统自检，和等待上位机发送信息包，若UART或USB收到正确的数据包，则发送中断标志，处理上位机发送过来的指令，一般为启动RFID操作标签流程。若UART或USB没有接收到有效的命令，则继续循环等待。

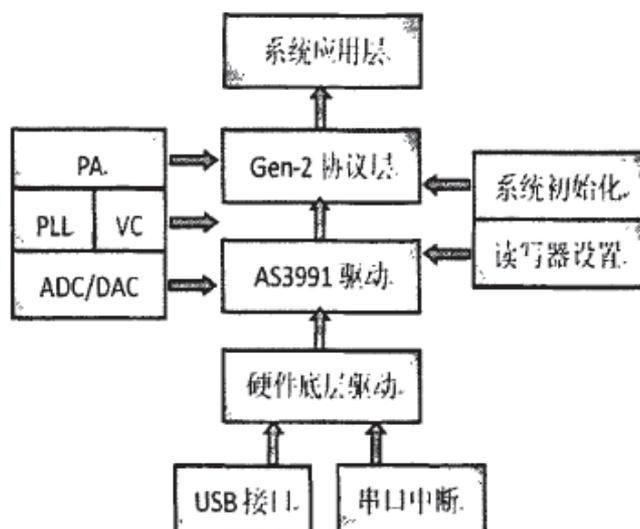


图5-1 系统程序结构

本系统RFID读写器程序结构如图5-1所示。系统应用层运行相关应用程序，在本设计中，集中表现为UART串口通信程序。协议层初始化读写器通信协议，包括ISO18000 6B和EPC Gen2，确定调制编码方式和数据格式。AS399x驱动包括初始化32个芯片寄存器和包括内部VCO和PLL、内部PA等在内的所有工作模块。硬件底层驱动包括初始化串口和USB口，以及相关底层硬件。

5.2 系统程序设计与实现

5.2.1 总体流程

底层软件主要是PC机通过USB接口、串口等接口与上位机进行数据交换，对读写器进行读标签信息、读标签或寄存器数据、写标签或寄存器数据、上锁 / 解锁、灭活标签等操作。

MCU作为阅读器的控制中枢，一方面要协调各个模块之间的工作，一方面要完成对通信协议的控制，它的工作流程如图5-2所示。在Main.C()主程序中，首先初始化MCU系统时钟、USB、UART，之后对AS399x芯片内部寄存器进行初始化，设定编码调制方式、工作频率、发射功率等参数。在MCU和射频芯片都初始化成功后，系统进行自测，通过调用uartCommands()函数判断上位机是否发来命令。如果没有，则继续自测；如果有发来命令，则判断是什么命令并执行相关操作。

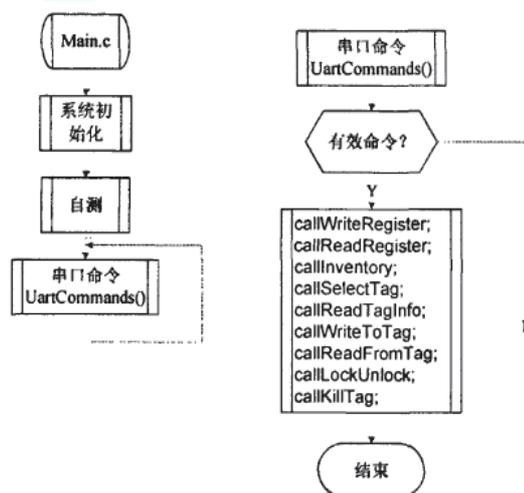


图5-2 程序流程图

5.2.2 系统防冲突算法

本系统防冲突算法使用EPC标准的概率分槽防冲突算法。根据EPC Gen2通信协议，其防冲突算法的流程是：首先读写器开始一个查询周期，向标签群发送一个Query()命令，在这个命令中包含一个参数Q(Q为0~15之间的整数)，当处于射频场内的标签群收到此命令后便会产生一个0至 2^Q-1 之间的随机数，并将此随机数放入槽计数器中。之后，读写器接收到标签的应答情况可以分为三种：第一种情况：若刚好某一个标签中的槽计数器值为0，则该标签反向散射其RN16给读写器，进行应答，没有碰撞发生；第二种情况：若没有标签的槽计数器值是0，则没有标签散射RN16，该时隙是空时隙。这时读写器将发送QueryRepO命令把标签群的槽计数器中的值减1，直到某个标签的槽计数器中的值为0，之后进行应答；第三种情况是：若有两个或两个以上的标签的槽计数器中的值同时为0，则这些标签会同时向读写器散射其RN16，这时射频场内产生了冲突。当有冲突产生时，在下一轮搜索中读写器会通过QueryAdjust0命令把Q值动态地加1或者减1，标签群根据新的Q值重新生成随机数进行应道，从而解决标签应答时的冲突问题。

从EPC标准规定的防冲突算法中可以看出，Q值越大，标签载入其槽计数器中的数值的范围就越大，从而标签所选的随机数相同的概率就越小，发生冲突的可能性也就越小，但由于搜索数量增多，收敛速度就会越慢；相反，Q值越小，标签发生冲突的可能性越大，但算法收敛速度越快。为提高工作效率，读写器需要在每一轮寻卡过程中动态地调整Q值，以便使槽计数器中的值获得最合适的取值范围。

如图5.3所示，在每一次搜索中，会出现三种情况：

1. 如果有且只有一张电子标签被正确识别，success计数器加1；
2. 如果有一张以上的电子标签同时回答，则说明产生了冲突，记录冲突的次数collision；
3. 如果没有电子标签作出回答，说明该时隙为空时隙，计数器null加1。

这里不妨假设每一次发生冲突时候，冲突的标签数都是2张，则在执行了一轮 2^Q-1 次搜索之后，判断正确识别标签的张数与两倍冲突次数之和是否大于 2^Q-1 （即 $suce+2 \times colli > 2^Q-1$ ），如果是，则说明射频场内的标签数目超过了目前Q值能容纳的最大数目，这时，使用QUERYADJUSTUP命令将Q值加1，再开始第二轮

搜索；否则，判断识别标签的张数与两倍冲突次数之和是否小于空时隙数(即 $succ+2 \times colli < null$)，如果是，说明Q值太大导致空时隙太多，增加了搜索时间，降低了搜索效率，使用QUERYADJUSTDOWN命令将Q值减1，再开始第二轮搜索；如果识别标签的张数与两倍冲突次数之和大于空时隙数而且小于 2^Q-1 ($null < succ+2 \times colli < 2^Q-1$)，说明Q值适当，不用调整。直到一轮搜索中colli计数器等于零时，退出标签搜索。

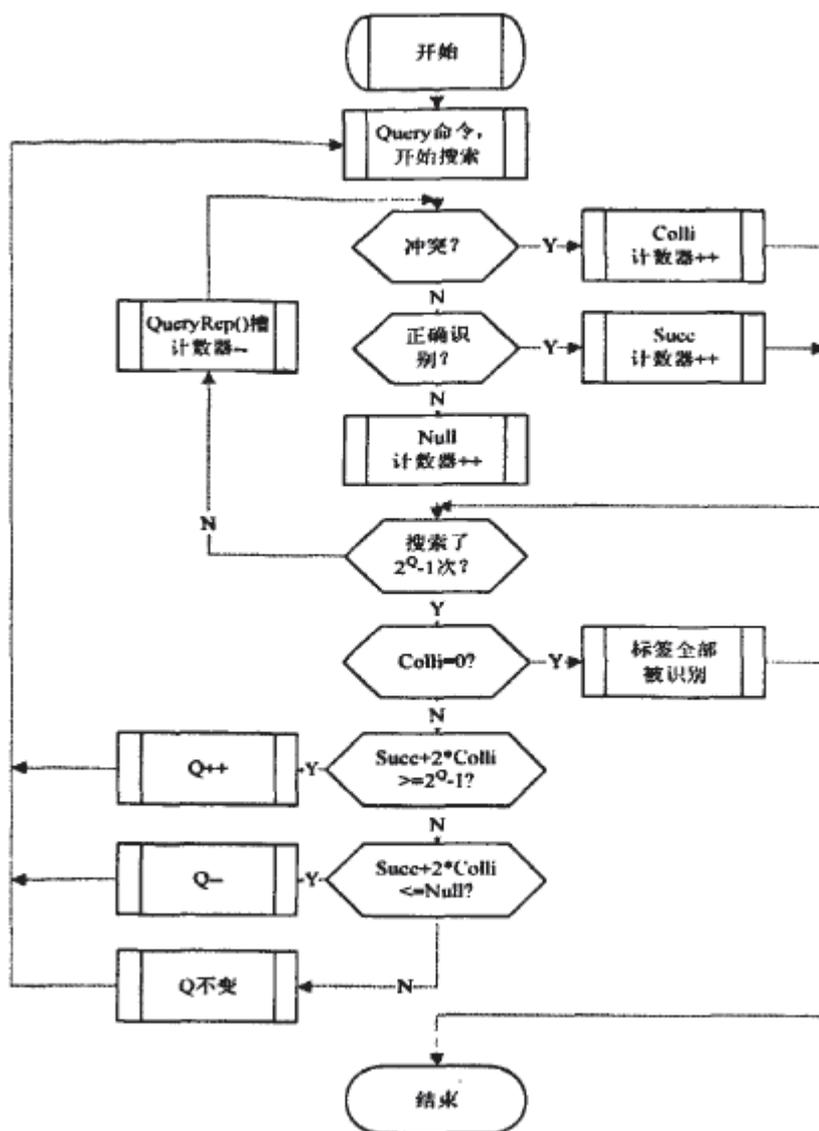


图5-3 Q值调整算法

5. 2. 3 写标签程序实现

读写器首先搜索射频范围内的电子标签，通过gen2SearchForTags函数()和gen2QueryStandard()函数唯一确定一张标签后，判断该标签是否设置了密码(即使用了Lock0命令的标签)，如果没有，则可以直接对选定的标签进行写操作；如果标签被锁定，读写器通过发送两条Access()和Req_RN(16)命令判定对该标签是否拥有写操作权限。

第一个Access()命令包含标签的以RN16异或高16位密码的访问口令，第二个Access()命令包含以不同的RN16异或低16位密码的访问口令。在发出Access()命令之前，读写器首先发出一个Req_RN()命令获得一个新的RN16。只有当两次验证都通过，即32位密码正确时，读写器才有对该标签的写操作权限。

Req_RN命令产生的16位随机数RN16，与标签Access密码进行异或得到命令参数。如果用户想要获得Access密码，就必须拥有相同的用于加密的RN16随机数，否则，无法取得密码。这措施有效保护了密码的隐秘性和通信的安全性。

写标签数据流程图如下图5-4所示：

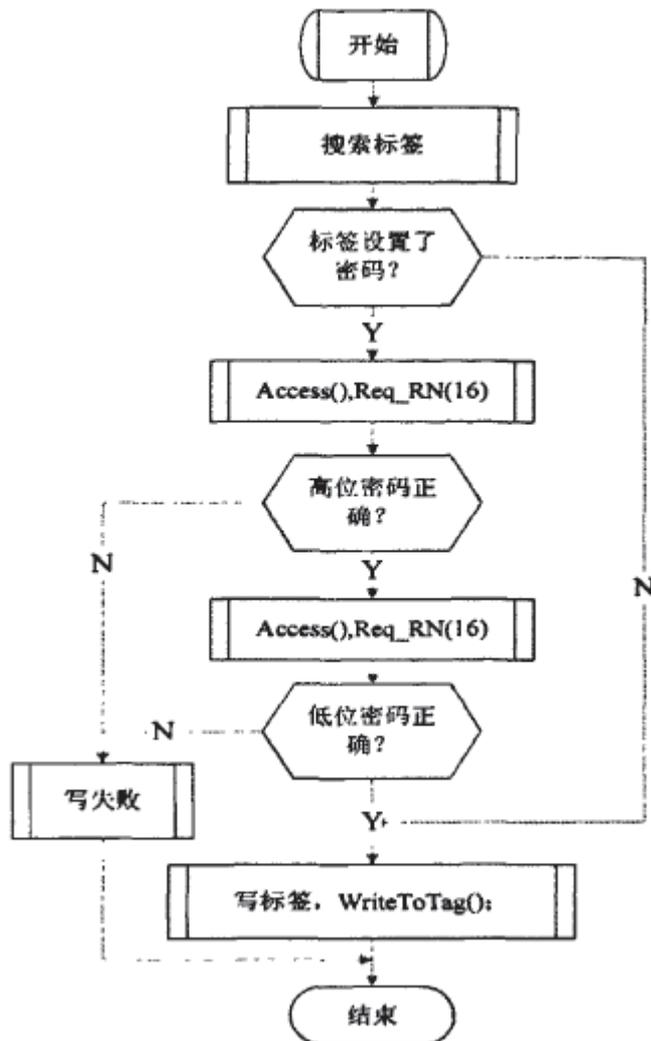


图5-4 写标签流程图

5.2.4 读标签程序实现

标签读操作可以分为单标签读和多标签读两种情况。

对于多标签读，就是同时出现多张电子标签，读写器要识别全部标签，而且不能出现重复读和漏读问题。多标签读主要应用在物流跟踪、门禁系统、货物识别等。大多数情况下天线范围内的物品都不止一件，例如门禁系统中，有可能在某一时刻有多个持卡人或者物品进出，这时正确唯一地把他们逐一识别出来，就需要更加复杂的算法以及更长的操作时间。

通过设置不同的Q值可以读取不同的标签数目。读写器一次可以识别 2^Q-1 张电子标签。当要识别的标签数大于 2^Q-1 时，一部分标签载入槽计数器的随机数必然相同，在连续收到QueryRep命令以及ACK命令之后，这些标签的随机数同

时减为0并同时返回应答信号，这时就会产生冲突。在实际的应用当中，事先不可能知道具体场合中标签的数量，所以没有办法准确地设置Q值。通过在识别过程中根据读标签过程的返回情况使用QueryAdjust命令修改Q值大小可以解决上面的问题。即根据射频场内不同的标签数目，自动调整Q值大小。

多标签读流程是：首先使用gen2SelectForTag()选择射频场内的标签群，之后通过含有Q值参数的gen2QueryStandard()命令对标签群启动一个盘存周期，之后不断发送QueryRep()命令和ACK()命令对标签槽计数器减值并进行识别，正确唯一识别的标签序列号被记录在存储器中。为了识别全部标签，QueryRep()命令和ACK()命令需要重复执行 $N=2^Q-1$ 次，即把所有Q值产生的可能的时隙都要历遍。多标签读流程如图5-5，在这个流程中，读写器需要根据每一轮搜索中标签的回波情况自动调整Q值大小，调整原理如章节5.2.2所述。如果标签已经被识别，则在接收到QueryRep()命令之后，退出之后的搜索过程。在一轮标签搜索中，如果没有读到标签，也没有发现冲突，则所有标签被识别，算法结束，退出标签的搜索过程。

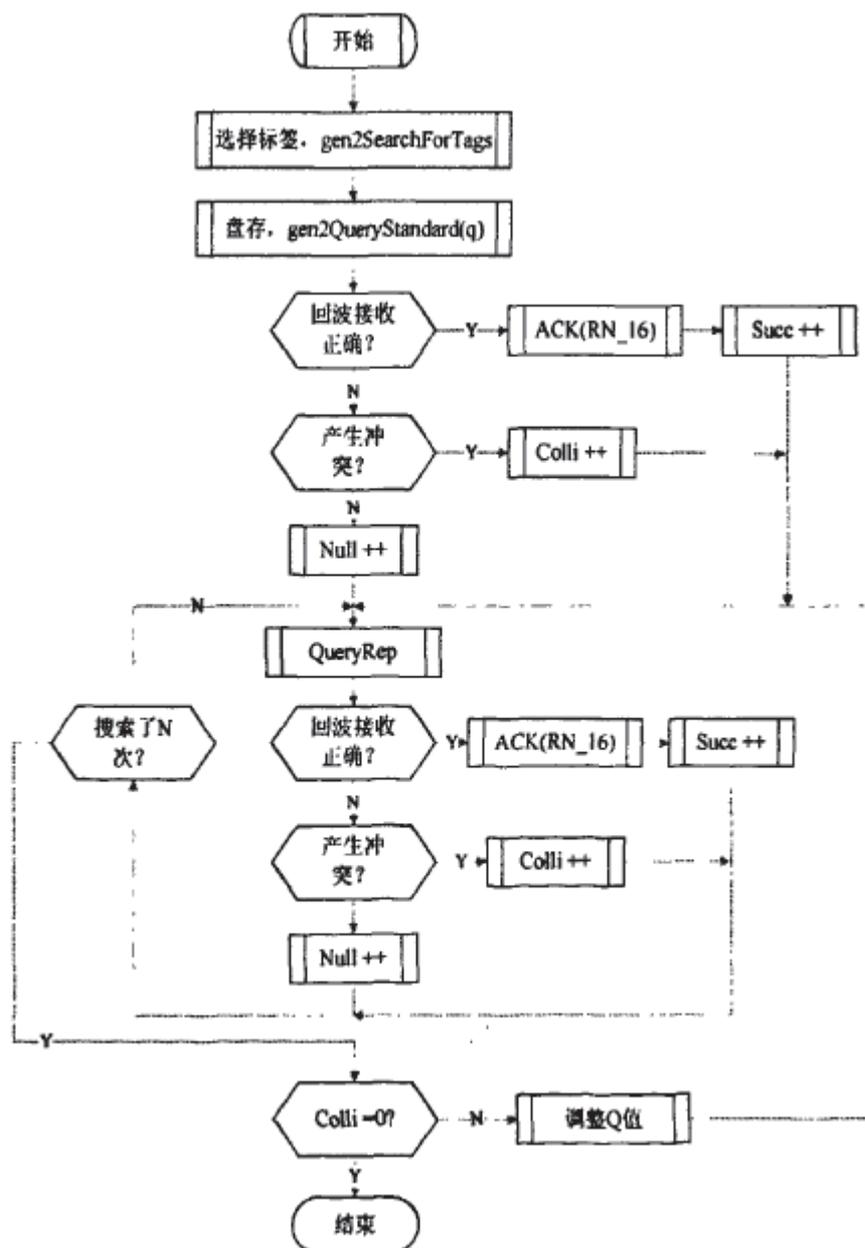


图5-5 多标签读流程图

单标签读是指读写器每次只需对单独一张标签进行识别，如果识别成功则马上停止搜索过程。身份识别、刷卡扣费、个别货物管理等应用中，就用到单标签读的功能。

对比多标签读，单表签读时间更快、算法也简单。由于单标签读在成功搜索到一张标签后则马上退出搜索过程。所以，单标签读可以设置Q值为0，这样，载入槽计数器的随机数必然等于0，即读写器只需搜索一次便可以把一张标签识

别出来，从而极大提高单标签读的速度。如图5-6所示，读写器通过UART接收到上位机读标签命令后，首先通过gen2SearchForTags()函数选择射频场内的一张标签。之后，gen2QueryStandard()函数确定了Q值大小，标签在 $0 \sim 2^Q - 1$ 范围内挑选一个随机数值(如果Q不等于0的时候)，并把该数值载入其槽计数器。如果该数值是零，标签则转换成应答状态，立即应答，反向散射RN16，并等待读写器用含有相同RN16的ACK进行确认，收到ACK后，标签进入确认状态，反向散射其PC、EPC和CRC16，之后通过gen2ReadFromTag()函数读出标签数据；如果槽计数器是非零数值，标签转换成仲裁状态，并等待之后发出的QueryRep()命令，把随机数不断减1，直到为零。

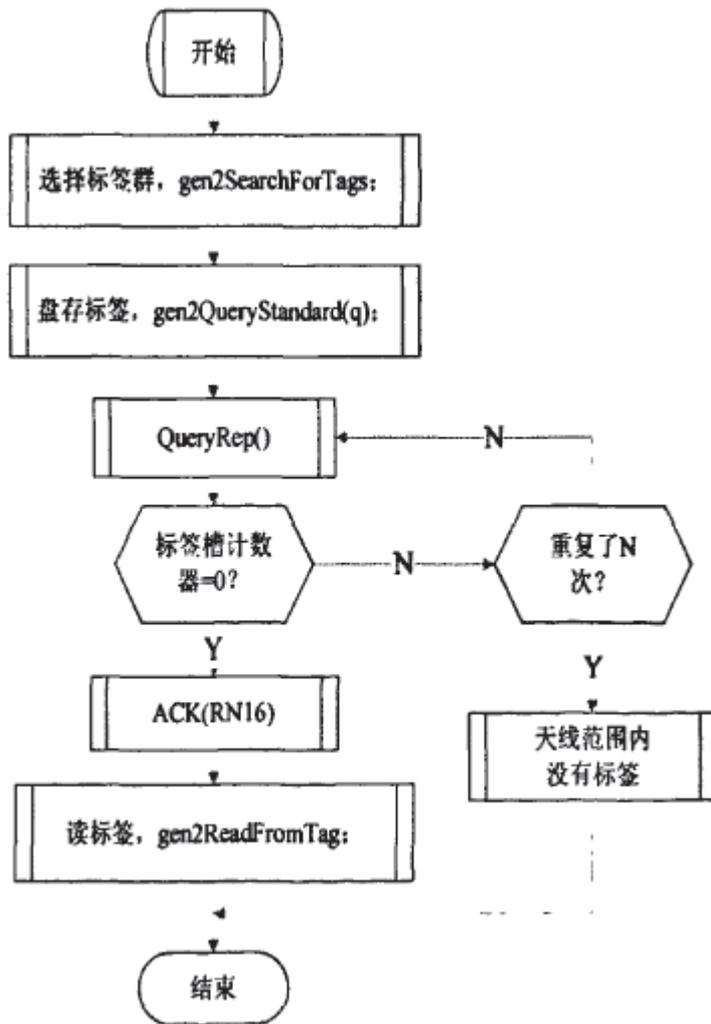


图5-6 单标签读流程图

5. 2. 5 锁标签程序实现

由于EPC Gen2标签是可写的，使用者可以任意修改标签的数据，这样就产生了信息安全问题：存储在标签内的数据可以被非法读取或者修改。为了保护合法用户的私有数据，EPC Gen2协议具有锁定标签的功能，即标签的指定的存储区是可锁定的。其中包括读锁定和写锁定，每种锁定又可以细分为暂时锁定或永久锁定，前者可以通过Access Password解锁，后者则无法解锁。用户可以通过标签锁定功能，将存放私有数据的区域根据实际需要进行读锁定或者写锁定。如果需要更改私有数据，可以使用Access Password进行解锁。

如图5-7所示，读写器首先发出gen2SearchForTags()命令选择一张天线范围内的标签。由于Access password长度是32位，需要通过连续两条的Req_RN(RN16)以及Access(Access password高/低位)命令，分别获得不同的RN16，并且和Access password异或进行验证，首先验证Access password的高16位，再验证Access password的低16位。如果回波正确，则使用gen2LockTag()命令对标签进行锁定；如果回波不正确，则锁标签操作失败，结束程序。

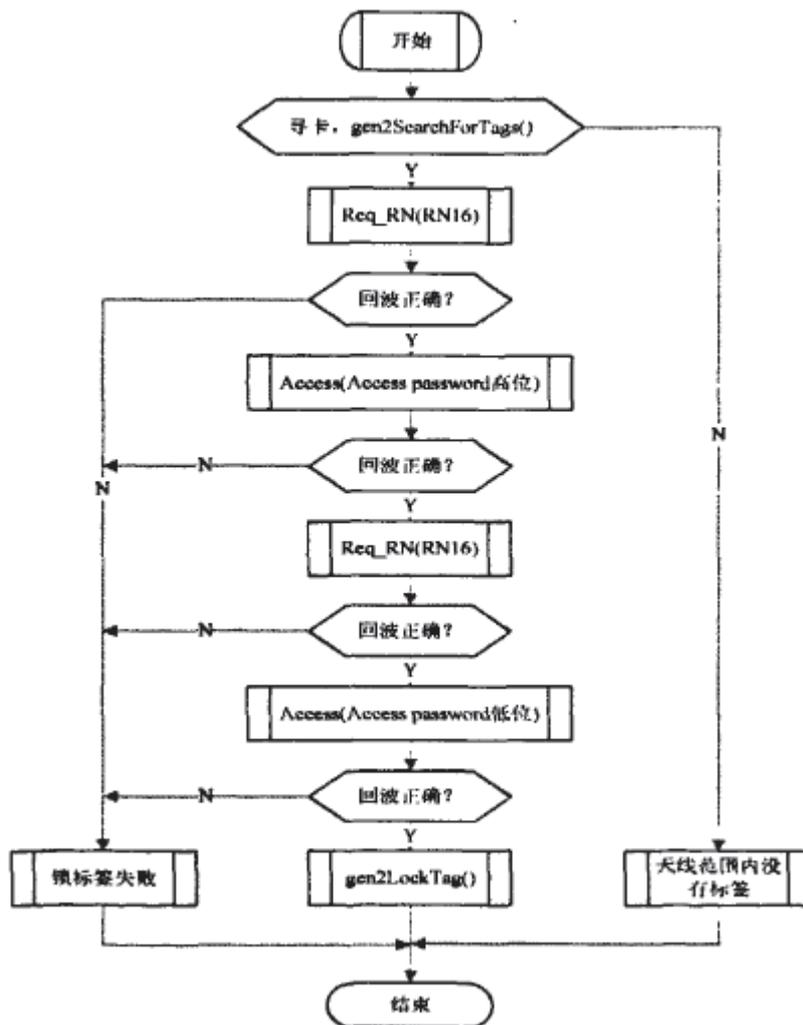


图5-7 锁标签流程图

5.2.6 灭活标签程序实现

灭活标签其实就是销毁标签。因为标签存储有大量信息，在退出使用时，销毁标签可以有效防止其内部信息被非法读取。销毁后，标签不再对任何命令作出反应，即内部数据无法再被读出。销毁标签功能在很多场合中都使用到，例如在服装贸易以及商品监控跟踪等领域上。随着RFID在物流零售业上应用的越来越广泛，很多的商品在售出后都要对贴附在商品上的标签进行销毁，销毁功能因此也相应地变得越来越重要。

如图5.8所示，读写器首先发出gen2SearchForTags()命令选择一张天线范围内的标签。和Access password一样，Kill password长度也是32位，所以同样需要

两个RN16分别与Kill password的高低位进行异或验证，具体流程也和锁标签相似。在灭活操作成功后，标签马上进入沉默状态，此后不再对读写器作任何应答；如果没有成功，读写器可以发出一个含标签句柄的Reel RN命令，以验证该标签仍然处于读写器的天线范围内，并可以再次启动如图5-8所示的多个步骤灭活程序。

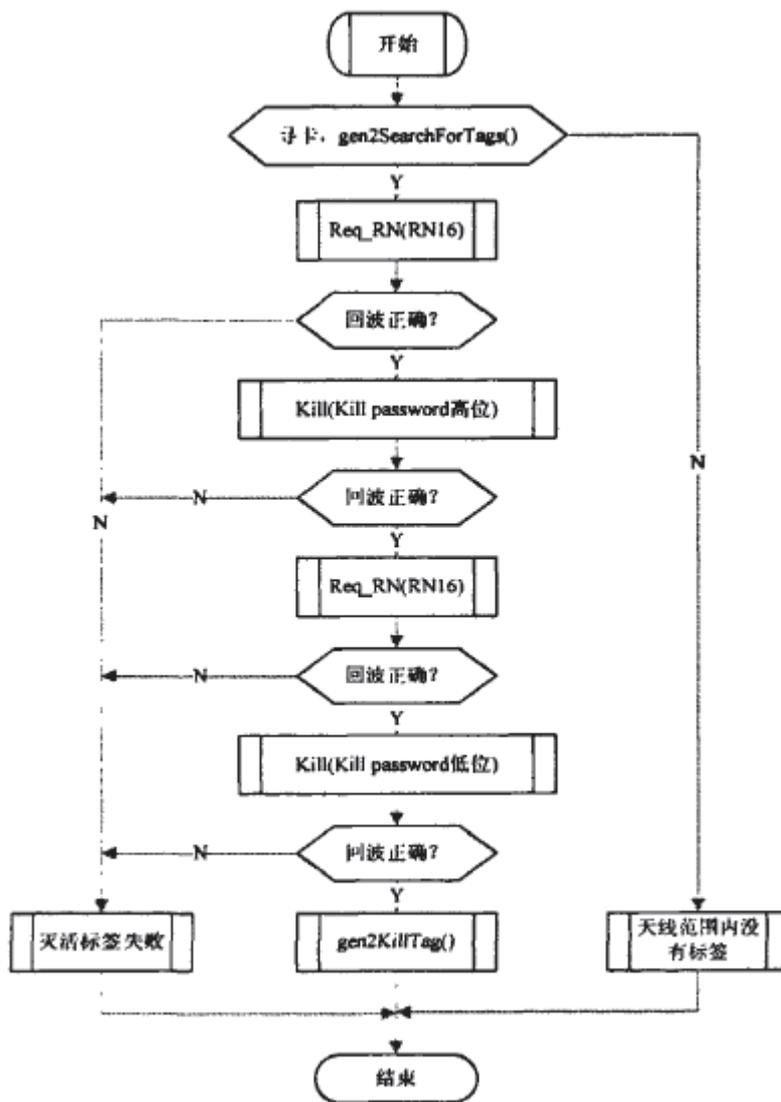


图5-8 灭活标签流程图

5.3 系统通信数据格式

标签存储器分成4个单独的块，每个块因为存储的数据内容不同而其功能也不尽相同，容量都是以字为单位。标签存储器的逻辑结构如图5-9所示：

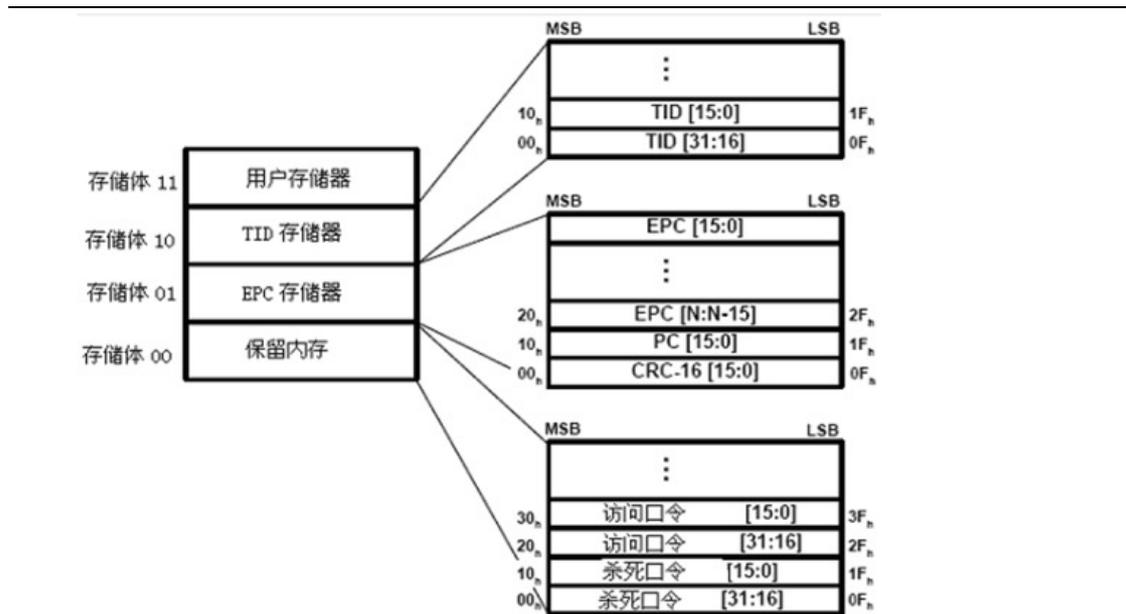


图5-9 标签存储器结构

1. Reserved块

保存标签两个长度为32位的密码：访问密码 (Access Password) 以及销毁密码 (Kill Password)。Access Password用于已经识别而且被锁定的标签的访问操作，只有验证Access Password正确，读写器才可以对标签进行相关访问操作；Kill Password用于标签销毁操作时的密码验证，同样地，只有销毁密码验证成功的标签才能被销毁。Reserved块的其他存储单元没有确定。

2. EPC块

包括EPC、PC和CRC-16。EPC是长度是96位的电子产品代码，即标签的序列号。PC位包含了标签相应的物理层基本信息。CRC-16用于数据完整性校验。

3. TID块

存储64位标签识别码。作为区分不同标签，每个TID码应该是唯一的。

4. User块

保存用户数据，本块的长度可变。

5. 3. 1 系统命令

通过PC的串口发送控制命令到读写器系统，读写器系统根据不同命令，访问标签不同的存储块，返回相应数据。主要命令如下表所示：

Report	value		Report	value
OUT_FIRM_HARDW_ID	0x10		OUT_KILL_TAG	0x3D
IN_FIRM_HARDW_ID	0x11		IN_KILL_TAG	0x3E
OUT_DEVICE_INFO	0x12		OUT_INVENTORY_6B_ID	0x3F
IN_DEVICE_INFO	0x13		IN_INVENTORY_6B_ID	0x40
OUT_CPU_RESET	0x16		OUT_CHANGE_FREQ	0x41
OUT_ANTENNA_POWER	0x18		IN_CHANGE_FREQ	0x42
OUT_WRITE_REG	0x1A		OUT_INVENTORY_RSSI	0x43
IN_WRITE_REG	0x1B		IN_INVENTORY_RSSI	0x44
OUT_READ_REG	0x1C		OUT_NXP_COMMAND	0x45
IN_READ_REG	0x1D		IN_NXP_COMMAND	0x46
OUT_INVENTORY	0x31		OUT_WRITE_TO_TAG_6B_ID	0x47
IN_INVENTORY	0x32		IN_WRITE_TO_TAG_6B_ID	0x48
OUT_SELECT_TAG	0x33		OUT_READ_FROM_TAG_6B_ID	0x49
IN_SELECT_TAG	0x34		IN_READ_FROM_TAG_6B_ID	0x50
OUT_WRITE_TO_TAG	0x35		OUT_FIRM_PROGRAM_ID	0x55
IN_WRITE_TO_TAG	0x36		IN_FIRM_PROGRAM_ID	0x56
OUT_READ_FROM_TAG	0x37		OUT_REGS_COMPLETE_ID	0x57
IN_READ_FROM_TAG	0x38		IN_REGS_COMPLETE_ID	0x58
OUT_LOCK_UNLOCK	0x3B		OUT_GEN2_SETTINGS_ID	0x59
IN_LOCK_UNLOCK	0x3C		IN_GEN2_SETTINGS_ID	0x5a

5.3.2 命令帧及数据帧结构

系统命令帧格式如下图5-10所示。主要包括三部分：

1. 帧头：即系统的控制命令，如表5.1所示。
2. 帧长度：整个命令帧的长度，包括帧头和数据部分。
3. 数据：读写的数据。

Byte 1	Byte 2	Variable length
Report ID	Frame Length	Payload

图5-10 系统命令帧格式

注：具体命令可见指令集。

Eleckits