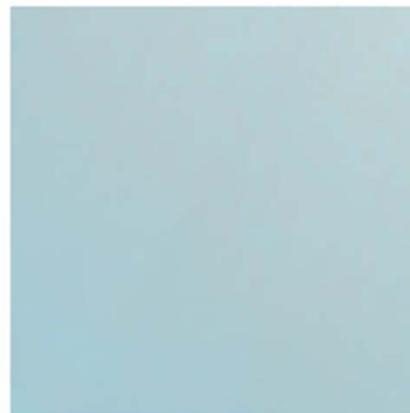


第2章 自动识别技术 与RFID

物联网导论

Introduction to Internet of Things





Introduction to Internet of Things



感知识别技术融合物理世界和信息世界，是物联网区别于其他网络最独特的部分。

本篇从**自动识别技术与RFID**开始，逐一介绍多样化的信息生成方式。

内容提要



内容回顾

- 第1章介绍了物联网的基本概念，核心技术，主要特点和应用前景。把物联网分为感知识别层、网络构建层、管理服务层和综合应用层四层。
- 本章介绍自动识别技术和RFID，重点讨论RFID组成，分类等，并简要介绍防止RFID标签冲突算法。



本章内容

2.1 自动识别技术

2.2 RFID的历史和现状

2.3 RFID技术分析

2.4 RFID标签冲突*

2.5 RFID和物联网

自动识别技术是模式识别理论的典型应用，选取不同的特征产生了多样的自动识别技术。





☑ 光符号识别&语音识别

光学字符识别（Optical Character Recognition, OCR），是模式识别（Pattern Recognition, PR）的一种技术，目的是要使计算机知道它到底看到了什么，尤其是文字资料。OCR技术能使设备通过光学机制识别字符。

语音识别研究如何采用数字信号处理技术自动提取及决定语言信号中最基本有意义的信息，同时也包括利用音律特征等个人特征识别说话人。

自动识别技术举例

光符号识别

语音识别

虹膜识别

指纹识别

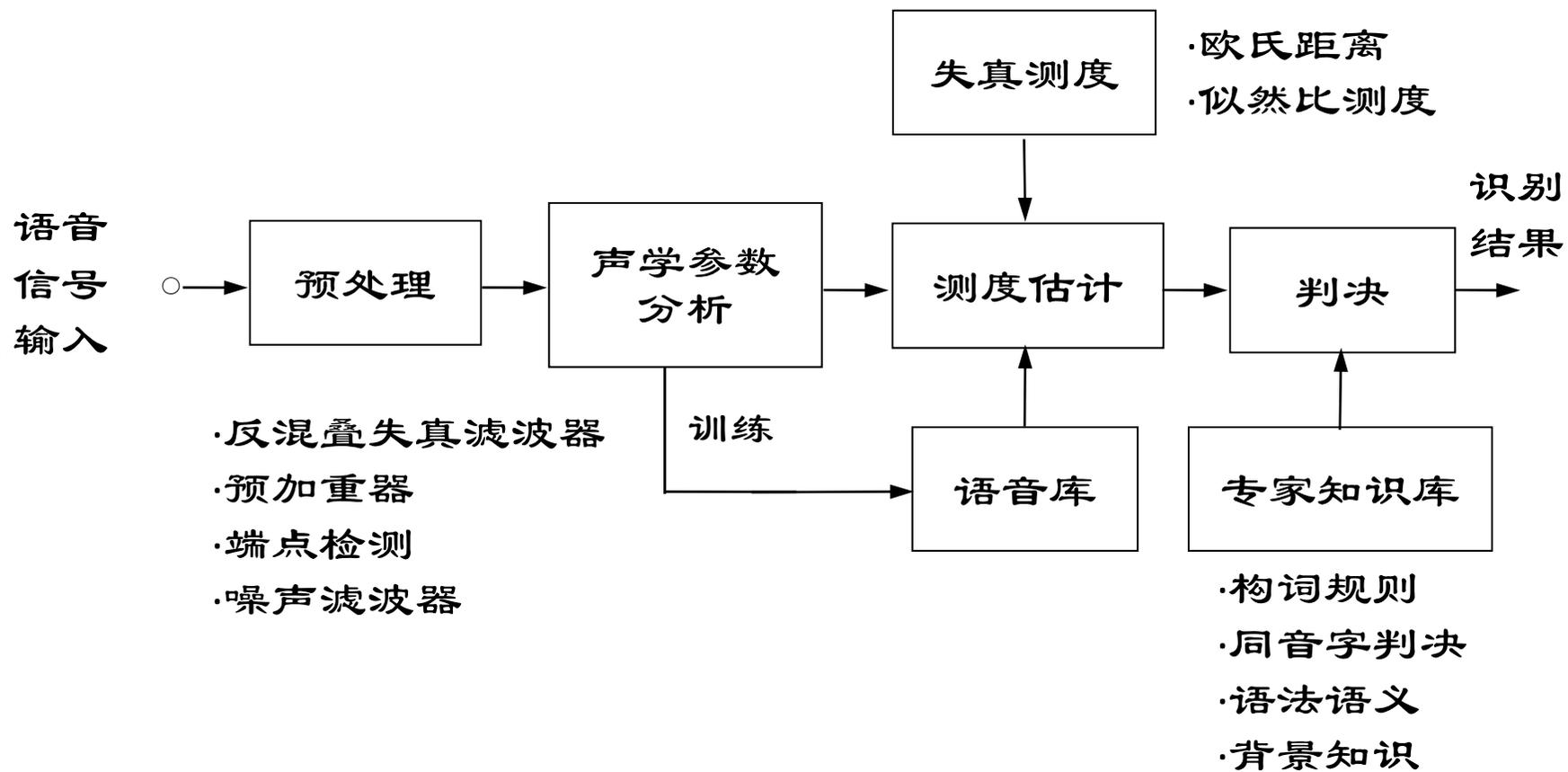
IC卡

条形码





语音识别框架：典型的模式识别系统





✓ 虹膜识别：合适的生物特征

虹膜识别是当前应用最方便精确的生物识别技术，虹膜的高度独特性和稳定性是其用于身份鉴别的基础。

虹膜识别的特点：

- **生物活性**：虹膜处在巩膜的保护下，生物活性强。
- **非接触性**：从无需用户接触设备,对人身没有侵犯。
- **唯一性**：形态完全相同虹膜的可能性低于其他组织。
- **稳定性**：虹膜定型后终身不变，一般疾病不会对虹膜组织造成损伤。
- **防伪性**：不可能在对视觉无严重影响的情况下用外科手术改变虹膜特征。

自动识别技术举例

光符号识别

语音识别

虹膜识别

指纹识别

IC卡

条形码





✔ 指纹识别技术

从实用角度看，**指纹识别**是优于其他生物识别技术的身份鉴别方法。因为指纹具有各不相同、终生基本不变的特点，且目前的指纹识别系统已达到操作方便、准确可靠、价格适中的阶段，正逐步应用于民用市场。

指纹识别的处理流程：

通过特殊的光电转换设备和计算机图像处理技术，对活体指纹进行采集、分析和比对，可以迅速、准确地鉴别出个人身份。系统一般主要包括对指纹图像采集、指纹图像处理、特征提取、特征值的比对与匹配等过程。

自动识别技术举例

光符号识别

语音识别

虹膜识别

指纹识别

IC卡

条形码





Q 指纹特征有哪些（总体特征）？

模式区：指纹上包含总体特征的区域，即从模式区就能够分辨出指纹是属于那一种类型的

纹数：模式区内指纹纹路的数量。



纹型：三种基本纹型包括：环型、弓型和螺旋型

三角点：位于从核心点开始的第一个分叉点或断点、或者两条纹路会聚处、孤立点、转折点、或者指向这些奇异点。



Q 指纹特征有哪些（局部特征）？



终结点 (Ending)：一条纹路在此终结。



分叉点 (Bifurcation)：一条纹路在此分开成为两条或更多的纹路。



分歧点 (Ridge Divergence)：两条平行的纹路在此分开。



孤立点 (Dot or Island)：一条特别短的纹路，以至成为一点。



环点 (Enclosure)：一条纹路分开成为两条之后，立即有合并成为一条，这样形成的一个小环称为环点。



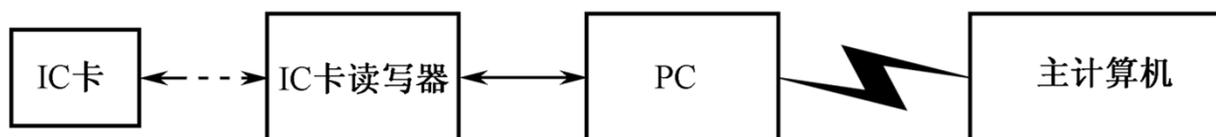
短纹 (Short Ridge)：一端较短但不至于成为一点的纹路。



✓ IC卡技术

IC卡 (Integrated Circuit Card)，即“集成电路卡”在 日常生活中已随处可见。实际上是一种数据存储系统， 如有必要还可附加计算能力。

一个标准的IC卡应用系统通常包括：IC卡、IC卡接口 设备 (IC卡读写器)、PC，较大的系统还包括通信 网络和主计算机等，如图所示。



自动识别技术举例

光符号识别

语音识别

虹膜识别

指纹识别

IC卡

条形码





✓ IC卡：基本组成

IC卡：由持卡人掌管，记录持卡人特征代码、文件资料的便携式信息载体。

接口设备：即IC卡读写器，是卡与PC信息交换的桥梁，且常是IC卡的能量来源。核心为可靠的工业控制单片机，如Intel的51系列等。

PC：系统的核心，完成信息处理、报表生成输出和指令发放、系统监控管理以及卡的发行与挂失、黑名单的建立等。

网络与计算机：通常用于金融服务等较大的系统。

自动识别技术举例

光符号识别

语音识别

虹膜识别

指纹识别

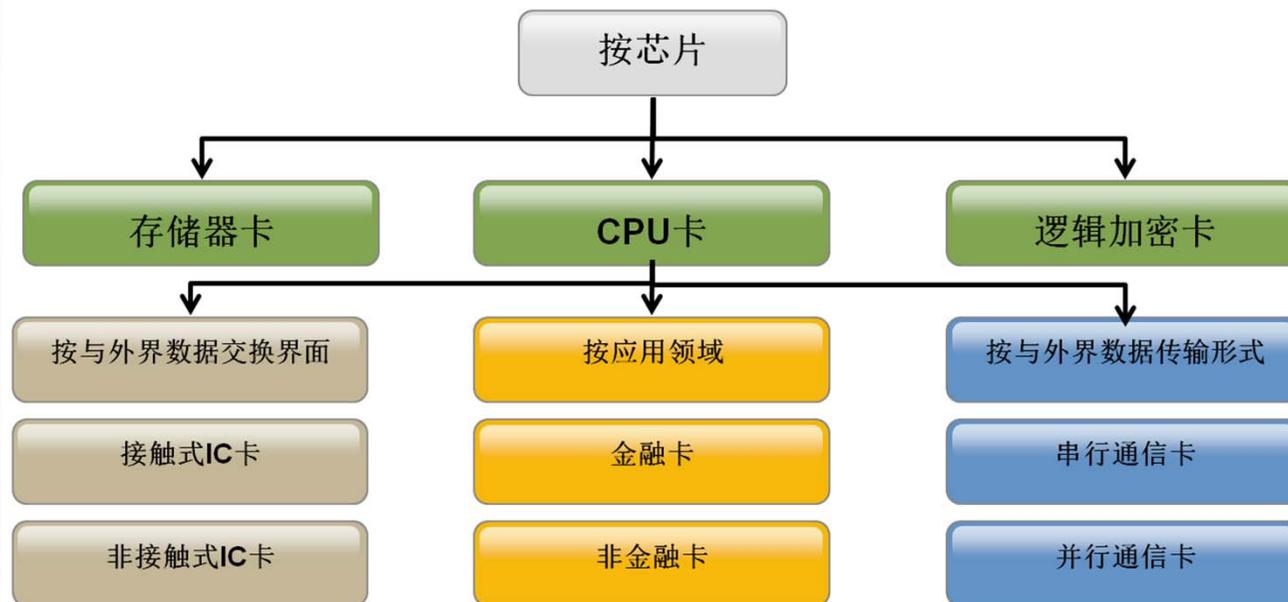
IC卡

条形码





☑ IC卡：分类



自动识别技术举例

光符号识别

语音识别

虹膜识别

指纹识别

IC卡

条形码





☑ IC卡：按芯片分类

(1) 存储器卡。存储器卡卡内嵌入的芯片为存储器芯片，这些芯片多为通用E2PROM（或Flash Memory）；无安全逻辑，可对片内信息不受限制地任意存取；卡片制造中也很少采取安全保护措施；不完全符合或支持ISO/IEC 7816国际标准，而多采用两线串行通信协议（I2C总线协议）或3线串行通信协议。

特点：

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



☑ IC卡：按芯片分类

(2) 逻辑加密卡。逻辑加密卡由非易失性存储器和硬件加密逻辑构成，一般是专门为IC卡设计的芯片，具有安全控制逻辑，安全性能较好；同时采用ROM、PROM、E2PROM等存储技术；从芯片制造到交货，均采取较好的安全保护措施，如运输密码TC（Transport Card）的取用；支持ISO/IEC 7816国际标准。

特点：

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



☑ IC卡：按芯片分类

(3) CPU卡。 CPU卡也称智能卡。CPU卡的硬件构成包括CPU、存储器（含RAM、ROM、E2PROM等）、卡与读写终端通信的I/O接口及加密运算协处理器CAU，ROM中则存放有COS（Chip Operation System，片内操作系统）。

特点：

- ① 计算能力高，存储容量大，应用灵活，适应性较强。
- ② 安全防伪能力强。不仅可验证卡和持卡人的合法性，且可鉴别读写终端，已成为一卡多用及对数据安全保密性特别敏感场合的最佳选择，如手机SIM卡等。
- ③ 真正意义上的“智能卡”。



☑ CPU卡：按交换界面分类

- 接触式IC卡



卡触点

- 非接触式IC卡



接触式IC卡的多个金属触点为卡芯片与外界的信息传输媒介，成本低，实施相对简便；非接触式IC卡则不用触点，而是借助无线收发传送信息，因此在前者难以胜任的交通运输等诸多场合有较多应用。



☑ CPU卡：按应用领域分类

根据应用领域的不同可将智能卡分为**金融卡和非金融卡（即银行卡和非银行卡）**。金融卡又分为信用卡和现金卡。前者用于消费支付时，可按预先设定额度透支资金，后者可用做电子钱包和电子存折，但不得透支。而非金融卡的涉及范围极广，实质上囊括了金融卡之外的所有领域，如门禁卡、组织代码卡、医疗卡、保险卡、IC卡身份证、电子标签等。



☑ CPU卡：按数据传输形式分类

根据与外界数据传输形式的不同可将智能卡分为串行通信卡和并行通信卡。串行通信卡即为目前最常用的卡，也是目前国际标准中所规定的接口方式。

采用串行方式与外界交换信息，卡芯片引脚较少，易于封装和接口。但随着芯片存储容量的增大，引发了两个问题：一是芯片面积急剧增长，给卡的封装带来困难；二是读写时间过长，读写1 MB的容量需要12分钟。

并行通信卡由于采用并行通信，故无此二弊，但国际标准中尚无此类接口标准。例如某种P型IC卡的引脚数多达32个，不仅速度极快，而且容量增大。与串行通信卡一样，它也有存储型、逻辑加密型和CPU型，并已在纳税申报等系统中得以应用。



✓ 条形码技术

条码技术是在计算机应用发展过程中，为消除数据录入的“瓶颈”问题而产生的，可以说是最“古老”的自动识别技术。

条形码是由一组规则排列的条、空以及对应的字符组成的标记。当使用专门的条形码识别设备如手持式条码扫描器扫描这些条码时，条码中包含的信息就转化为计算机可识别的数据。

目前市场上常见的是一维条形码，信息量约几十位数据和字符；二维条形码相对复杂，但信息量可达几千字符。

自动识别技术举例

光符号识别

语音识别

虹膜识别

指纹识别

IC卡

条形码





☑ 条形码技术：一维条形码

一维条码是由一组规则排列的条、空以及对应的字符组成的标记。普通的一维条码在使用过程中仅作为识别信息，它的意义是通过在计算机系统的数据库中提取相应的信息而实现的。

一个完整的条码的组成次序依次为：静区（前）、起始符、数据符、（中间分割符，主要用于EAN码）、(校验符)、终止符、静区（后）。



自动识别技术举例

光符号识别

语音识别

虹膜识别

指纹识别

IC卡

条形码





☑ 一维条形码：几个基本概念

模块：构成条码的基本单位是模块，模块是指条码中最窄的条或空，模块的宽度通常以mm或mil（千分之一英寸）为单位。构成条码的一个条或空称为一个单元，一个单元包含的模块数是由编码方式决定的，有些码制中，如EAN码，所有单元由一个或多个模块组成；而另一些码制，如39码中，所有单元只有两种宽度，即宽单元和窄单元，其中的窄单元即为一个模块。

密度（Density）：条码的密度指单位长度的条码所表示的字符个数。模块尺寸越小，密度越大，所以密度值通常以模块尺寸的值来表示（如5mil）。通常7.5mil以下的条码称为高密度条码，15mil以上的条码称为低密度条码。

宽窄比：对于只有两种宽度单元的码制，宽单元与窄单元的比值称为宽窄比，一般为2-3左右（常用的有2:1, 3:1）。宽窄比较大时，阅读设备更容易分辨宽单元和窄单元，因此比较容易阅读。



☑ 一维条形码：几个基本概念（续）

对比度（PCS）：条码符号的光学指标，PCS值越大则条码的光学特性越好

$$PCS = (RL - RD) / RL \times 100\%$$

（RL：条的反射率 RD：空的反射率）

条码长度：从条码起始符前缘到终止符后缘的长度

条码密度：单位长度的条码所表示的字符个数

双向条码：条码的两段都可以作为扫描起点的。

中间分隔符：在条码符号中，位于两个相邻的条码符号之间且不代表任何信息的空。

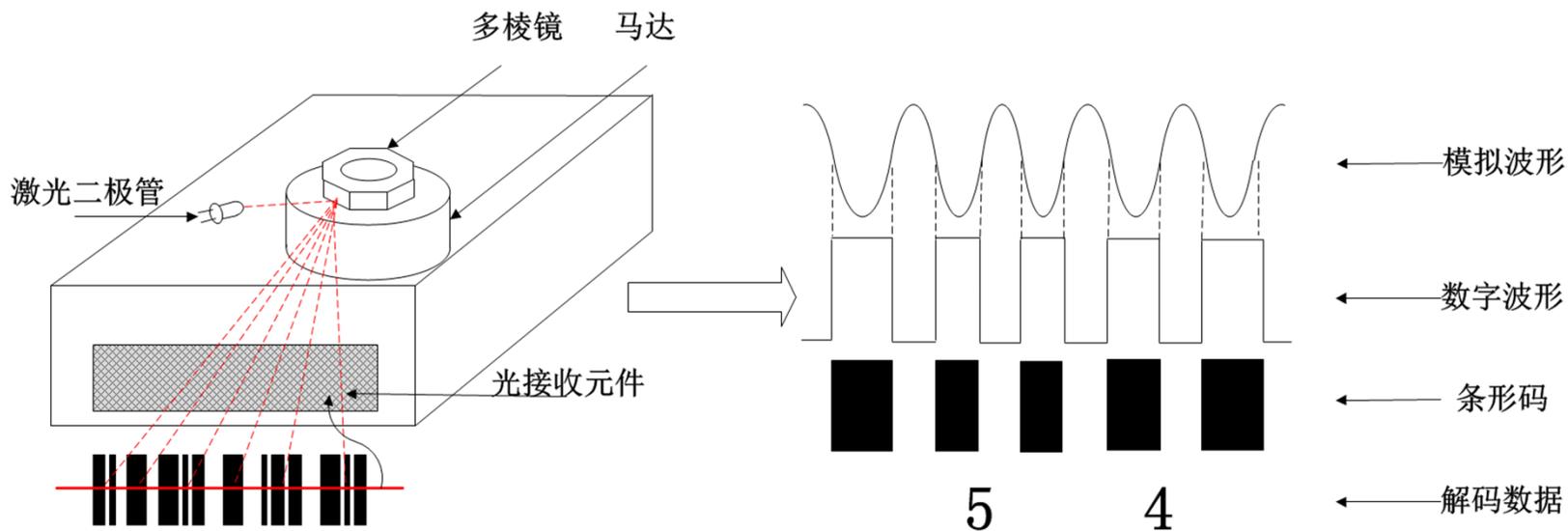
连续性条码：在条码字符中，两个相邻的条码字符之间没有中间分隔符的条码。

非连续性条码：在条码字符中，两个相邻的条码字符之间存在中间分隔符的条码。



☑ 一维条形码：译码原理

激光扫描仪通过一个激光二极管发出一束光线，照射到一个旋转的棱镜或来回摆动的镜子上，反射后的光线穿过阅读窗照射到条码表面，光线经过条或空的反射后返回阅读器，由一个镜子进行采集、聚焦，通过光电转换器转换成电信号，该信号将通过扫描期或终端上的译码软件进行译码。





☑ 一维条形码：典型一维条形码制比较

	UPC码	EAN码	交叉25码	39码	库德巴码	128码	93码	49码
长度	固定	固定	可变	可变	可变	可变	可变	可变
连续型	连续	连续	离散	离散	连续	连续	连续	连续
支持符号	数字式	数字式	自校验数字式	字母数字式	自校验数字式	自校验数字式	字母数字式	字母数字式
字符集	0-9	0~9	0-9、 A-Z 。 - / + %\$space	0-9 。 / + %—\$	0-9 : - / 。 + \$	ASC II 码	0~9、 A~Z o- / + %\$Space	0~9、A~Z 。 - / +% \$space F1、F2、F3 三个变换字符
元素宽度	四种	四种	两种	多种可变	多种可变	四种	多种可变	多种可变
应用领域	零售业 包装业	零售业 包装业	仓储 产品识别 包装识别 汽车工业	汽车业 工业界	仓库 血库 航空快递 包裹	工业 库存管理 运输配送		



✓ 条形码技术：二维条形码

二维码利用某种特定的几何图形按一定规律在平面（二维方向上）分布的黑白相间的图形记录数据符号信息的；在代码编制上巧妙地利用构成计算机内部逻辑基础的“0”、“1”比特流的概念，使用若干个与二进制相对应的几何形体来表示文字数值信息，通过图象输入设备或光电扫描设备自动识读以实现信息自动处理。

二维码具有条码技术的一些共性：每种码制有其特定的字符集；每个字符占有一定的宽度；具有一定的校验功能等。同时还具有对不同行的信息自动识别功能、及处理图形旋转变化等特点。

自动识别技术举例

光符号识别

语音识别

虹膜识别

指纹识别

IC卡

条形码





✓ 条形码技术：二维条形码

目前，世界上应用最多的二维条码符号有Aztec Code、PDF147、DataMatrix、QR Code、Code16K等。



Aztec Code



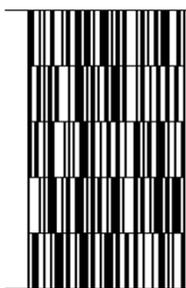
PDF147



QR Code



DataMatrix



Code 16K

自动识别技术举例

光符号识别

语音识别

虹膜识别

指纹识别

IC卡

条形码





☑ 一维条形码与二维条形码的比较

一维条形码特点:

1. 可直接显示内容为英文、数字、简单符号;
2. 贮存数据不多, 主要依靠计算机中的关联数据库;
3. 保密性能不高;
4. 损坏后可读性差。

二维条形码特点:

1. 可直接显示英文、中文、数字、符号、图型;
2. 贮存数据量大, 可存放1K字符, 可用扫描仪直接读取内容, 无需另接数据库;
3. 保密性高(可加密),
4. 安全级别最高时, 损坏50%仍可读取完整信息。



本章内容

2.1 自动识别技术

2.2 **RFID的历史和现状**

2.3 RFID技术分析

2.4 RFID标签冲突*

2.5 RFID和物联网

RFID对于计算机自动识别技术而言是一场革命，极大地提高了信息处理效率和准确度。





2.2 RFID的历史与现状

RFID是射频识别技术（Radio Frequency Identification）的英文缩写,利用射频信号通过空间耦合（交变磁场或电磁场）实现无接触信息传递并通过所传递的信息达到识别目的。

它是上世纪90年代兴起的自动识别技术，首先在欧洲市场上得以使用，随后在世界范围内普及。

RFID较其它技术明显的优点是电子标签和阅读器无需接触便可完成识别。射频识别技术改变了条形码依靠"有形"的一维或二维几何图案来提供信息的方式，通过芯片来提供存储在其中的数量巨大的"无形"信息。



2.2 RFID的历史与现状

年代	事件
1941-1950	雷达技术催生了RFID技术，1948年奠定了RFID技术的理论基础
1951-1960	早期RFID技术的探索阶段，仍处于实验室实验研究。
1961-1970	RFID技术的理论得到进一步发展，人们开始尝试一些新应用。
1971-1980	RFID技术与产品研发处于高潮期，各种RFID技术测试得到加速出现了最早的商业应用。
1981-1990	RFID技术及产品进入商业应用阶段，各种规模应用开始出现。
1991-2000	RFID技术标准化问题日趋得到重视，RFID应用更加丰富，已经成为人们生活中的一部分。
2000-至今	RFID产品种类更加丰富，各类标签得到大发展，标签的成本也不断降低，规模应用行业开始扩张。



2.2 RFID的历史与现状

目前RFID技术应用已经处于全面推广的阶段。特别是对于IT业而言，RFID技术被视为IT业的下一个“金矿”。各大软硬件厂商包括IBM、Motorola、Philips、TI、Microsoft、Oracle、Sun、BEA、SAP等在内的各家企业都对RFID技术及其应用表现出了浓厚的兴趣，相继投入大量研发经费，推出了各自的软件或硬件产品及系统应用解决方案。

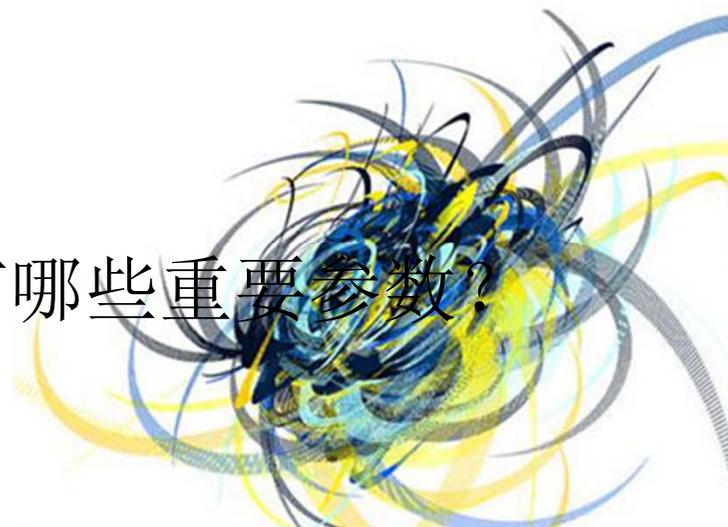
在应用领域，以Wal-Mart，UPS，Gillette等为代表的众多企业已经开始全面使用RFID技术对业务系统进行改造，以提高企业的工作效率、管理水平并为客户提供各种增值服务。



本章内容

- 2.1 自动识别技术
- 2.2 RFID的历史和现状
- 2.3 **RFID技术分析**
- 2.4 RFID标签冲突*
- 2.5 RFID和物联网

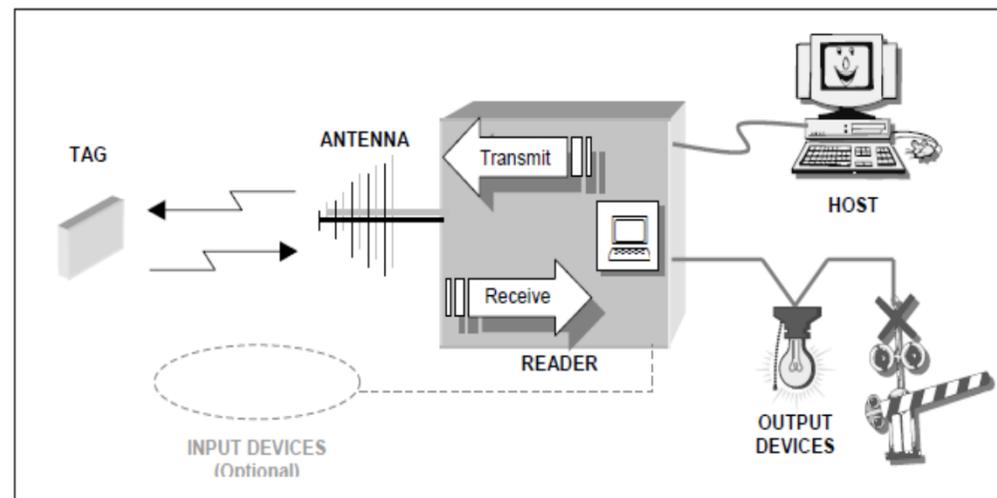
RFID系统的基本组成是什么？有哪些重要参数？





2.3 RFID技术分析

RFID系统由五个组件构成，包括：传送器、接收器、微处理器、天线、标签。传送器、接收器和微处理器通常都被封装在一起，又统称为阅读器(Reader)，所以工业界经常将RFID系统分为为阅读器、天线和标签三大组件，这三大组件一般都可由不同的生厂商生产。





2.3 RFID技术分析：阅读器

阅读器是RFID系统最重要也是最复杂的一个组件。因其工作模式一般是主动向标签询问标识信息，所以有时又被称为询问器（Interrogator）。下图显示不同类型的阅读器。阅读器可以通过标准网口、RS232串口或USB接口同主机相连，通过天线同RFID标签通信。有时为了方便，阅读器和天线以及智能终端设备会集成在一起形成可移动的手持式阅读器。





Introduction to Internet of Things

2.3 RFID技术分析：天线

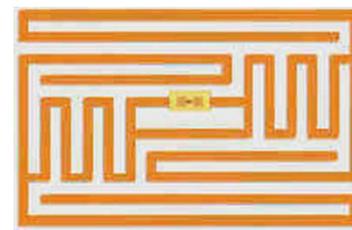
天线同阅读器相连，用于在标签和阅读器之间传递射频信号。阅读器可以连接一个或多个天线，但每次使用时只能激活一个天线。RFID系统的工作频率从低频到微波，这使得天线与标签芯片之间的匹配问题变得很复杂。





2.3 RFID技术分析：标签

标签（Tag）是由耦合元件、芯片及微型天线组成，每个标签内部存有唯一的电子编码，附着在物体上，用来标识目标对象。标签进入RFID阅读器扫描场以后，接收到阅读器发出的射频信号，凭借感应电流获得的能量发送出存储在芯片中的电子编码（被动式标签），或者主动发送某一频率的信号（主动式标签）。





☑ 标签：存储方式

电可擦可编程只读存储器（EEPROM）：一般射频识别系统主要采用EEPROM方式。这种方式的缺点是写入过程中的功耗消耗很大，使用寿命一般为100,000次

铁电随机存取存储器（FRAM）：与EEPROM相比，FRAM的写入功耗消耗减小100倍，写入时间甚至缩短1000倍。FRAM属于非易失类存储器。然而，FRAM由于生产方面的问题至今未获得广泛应用。

静态随机存取存储器（SRAM）：SRAM能快速写入数据，适用于微波系统，但SRAM需要辅助电池不间断供电，才能保存数据。



☑ 标签分类

被动式标签 (Passive Tag)：因内部没有电源设备又被称为无源标签。被动式标签内部的集成电路通过接收由阅读器发出的电磁波进行驱动，向阅读器发送数据。

主动标签 (Active Tag)：因标签内部携带电源又被称为有源标签。电源设备和与其相关的电路决定了主动式标签要比被动式标签体积大、价格昂贵。但主动标签通信距离更远，可达上百米远。

半主动标签 (Semi-active Tag)：这种标签兼有被动标签和主动标签的所有优点，内部携带电池，能够为标签内部计算提供电源。这种标签可以携带传感器，可用于检测环境参数，如温度、湿度、是否移动等。然而和主动式标签不同是它们的通信并不需要电池提供能量，而是像被动式标签一样通过阅读器发射的电磁波获取通信能量。



Q RFID标签与条形码相比的优点？

体积小且形状多样： RFID标签在读取上并不受尺寸大小与形状限制，不需要为了读取精度而配合纸张的固定尺寸和印刷品质。

耐环境性： 纸张容易被污染而影响识别。但RFID对水、油等物质却有极强的抗污性。另外，即使在黑暗的环境中，RFID标签也能够被读取。

可重复使用： 标签具有读写功能，电子数据可被反复覆盖，因此可以被回收而重复使用。

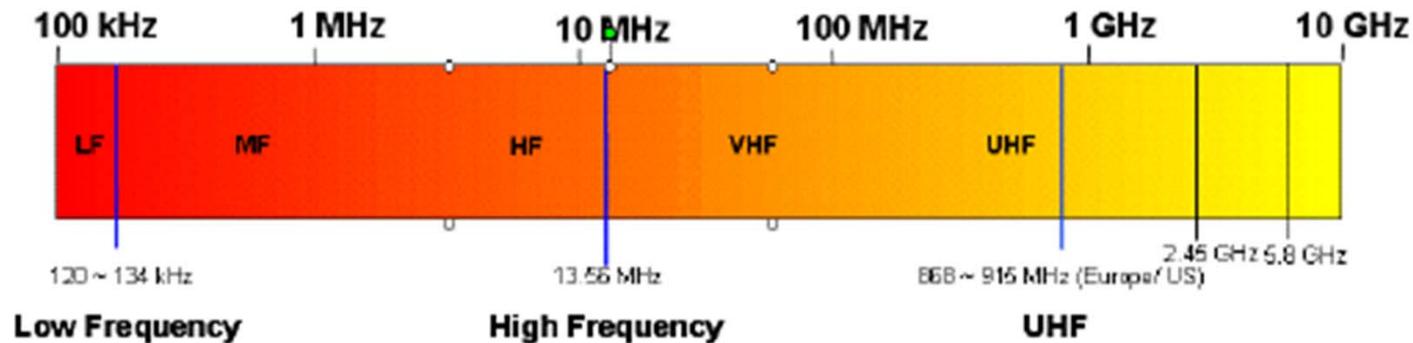
穿透性强： 标签在被纸张、木材和塑料等非金属或非透明的材质包裹的情况下也可以进行穿透性通讯。

数据安全性： 标签内的数据通过循环冗余校验的方法来保证标签发送的数据准确性。



2.3 RFID技术分析：频率

RFID频率是RFID系统的一个很重要的参数指标，它决定了工作原理、通信距离、设备成本、天线形状和应用领域等因素。RFID典型的工作频率有125KHz、133KHz、13.56MHz、27.12MHz、433MHz、860-960MHz、2.45GHz、5.8GHz等。按照工作频率的不同，RFID系统集中在低频、高频和超高频三个区域





✓ RFID频率

低频（LF）范围为30kHz-300kHz，RFID典型低频工作频率有125kHz和133kHz两个，该频段的波长大约为2500m。低频标签一般都为无源标签，其工作能量通过电感耦合的方式从阅读器耦合线圈的辐射场中获得，通信范围一般小于1米。除金属材料影响外，低频信号一般能够穿过任意材料的物品而不降低它的读取距离。

高频（HF）范围为3 MHz -30 MHz，RFID典型工作频率为13.56MHz,该频率的波长大概为22米，通信距离一般也小于1米。该频率的标签不再需要线圈绕制，可以通过腐蚀活字印刷的方式制作标签内的天线，采用电感耦合的方式从阅读器辐射场获取能量。



☑ RFID频率（续）

超高频（UHF）范围为300MHz-3GHz，3GHz以上为微波范围。采用超高频和微波的RFID系统一般统称为超高频RFID系统，典型的工作频率为：

433MHz，860-960MHz，2.45GHz，5.8GHz，频率波长大概在30厘米左右。

严格意义上，2.45GHz和5.8GHz属于微波范围。超高频标签可以是有源标签与无源标签两种，通过电磁耦合方式同阅读器通信。通信距离一般大于1米，典型情况为4-6米，最大可超过10米。



本章内容

2.1 自动识别技术

2.2 RFID的历史和现状

2.3 RFID技术分析

2.4 **RFID标签冲突***

2.5 RFID和物联网

多个标签同时处于阅读器识别范围之内或多个标签同时向阅读器发送标志信号时，将发生标签信号冲突。





2.4 RFID标签冲突

标签信号冲突：随着阅读器通信距离的增加其识别区域的面积也逐渐增大，这常常会引发多个标签同时处于阅读器的识别范围之内。但由于阅读器与所有标签共用一个无线通道，当两个以上的标签同一时刻向阅读器发送标识信号时，信号将产生叠加而导致阅读器不能正常解析标签发送的信号。这个问题通常被称为标签信号冲突问题（或碰撞问题），解决冲突问题的方法被称为防冲突算法（或防碰撞算法，反冲突算法）。

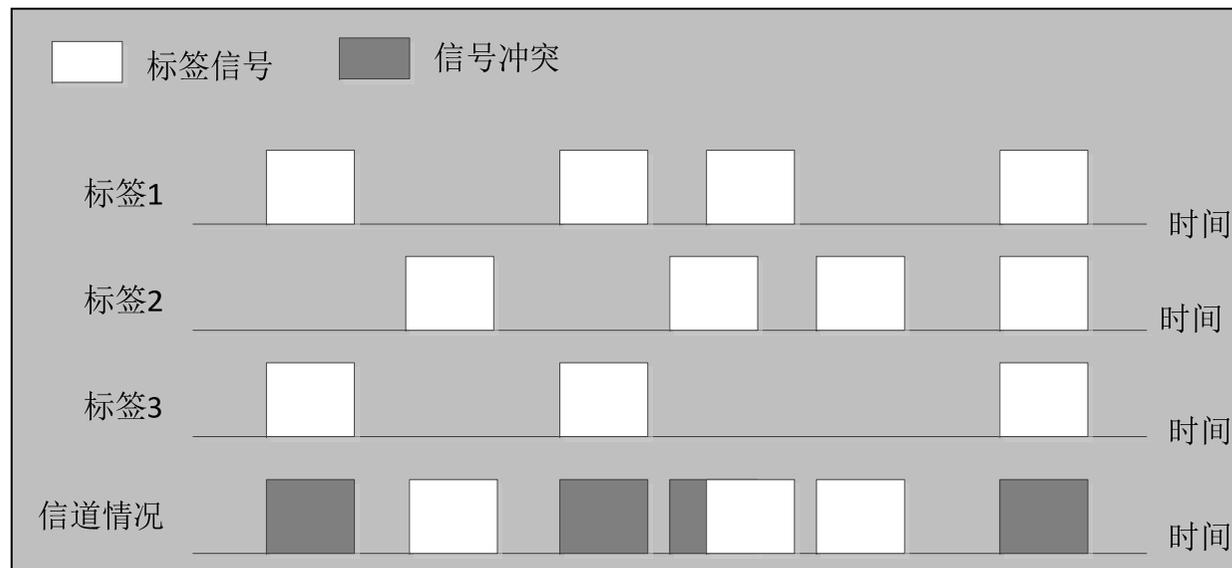
现有的基于时分多址防冲突算法可以分为基于ALOHA机制的算法和基于二进制树两种类型，而这两种类型又包括若干种变体。



基于ALOHA的防冲突算法

纯ALOHA防冲突算法

算法简单，易于实现，但信道利用率仅为18.4%，性能非常不理想。

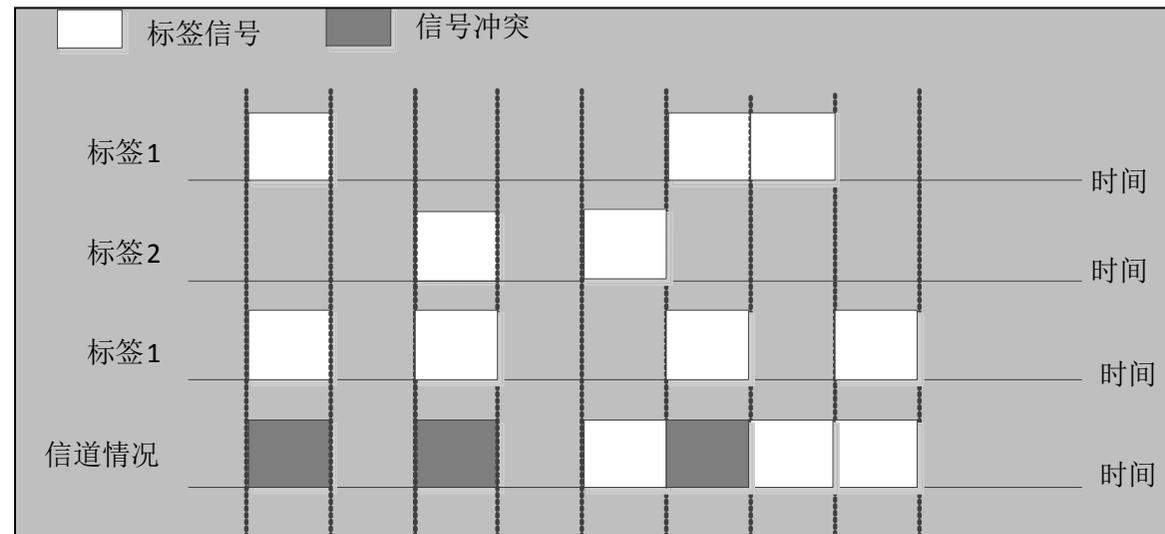




基于ALOHA的防冲突算法

分时隙的ALOHA防冲突算法 (S-ALOHA)

S-ALOHA算法将纯ALOHA算法的时间分为若干时隙，每个时隙大于或等于标签标识符发送的时间长度，并且每个标签只能在时隙开始时刻发送标识符。由于系统进行了时间同步，S-ALOHA协议的信道利用率达到36.8%，是纯ALOHA的两倍。

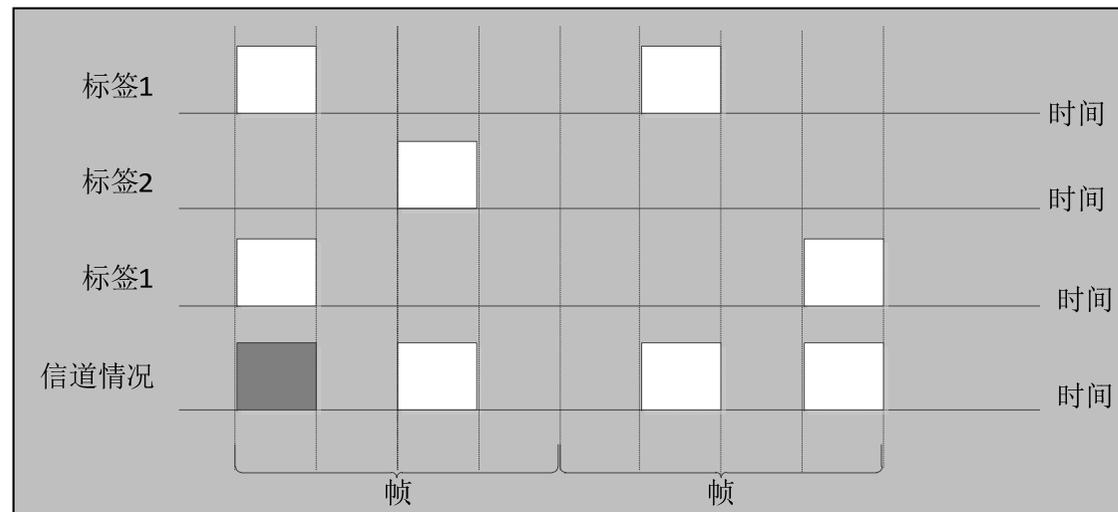




基于ALOHA的防冲突算法

基于帧的分时隙ALOHA防冲突算法 (FSA)

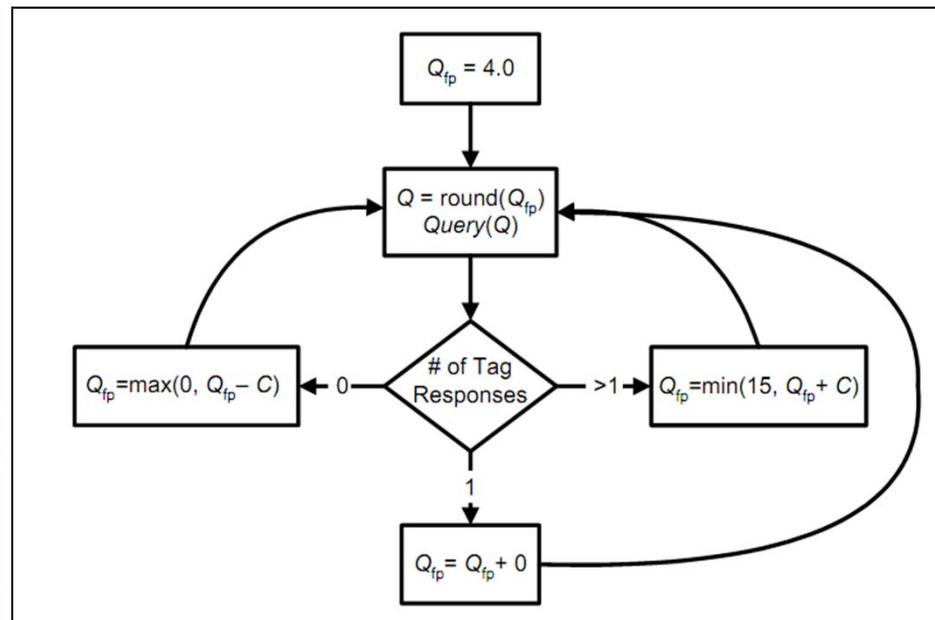
在S-ALOHA基础上，将若干个时隙组织为一帧，阅读器按照帧为单元进行识别。优点在于逻辑简单，电路设计简单，所需内存少，且在帧内只随机发送一次能够更进一步降低了冲突的概率。FSA成为RFID系统中最常用的一种基于ALOHA的防冲突算法。





基于ALOHA的防冲突算法

Q算法



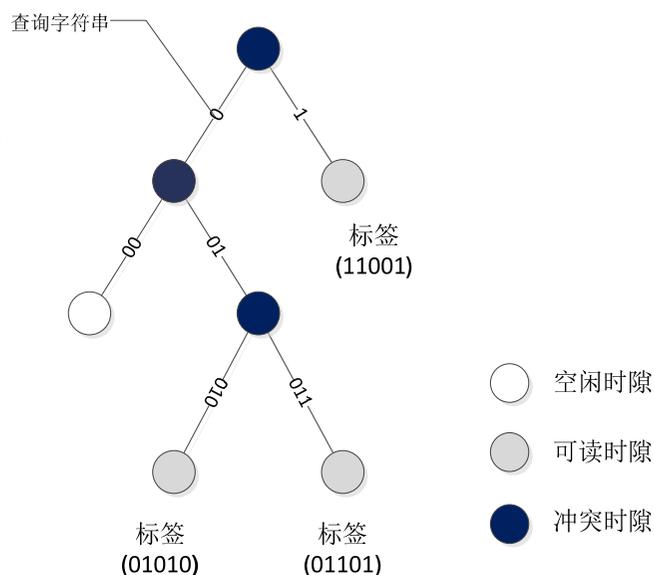
动态自适应设置帧长度的算法可以解决FAS算法固定帧的局限性。目前流行的方法有两种：一种根据前一帧通信获取的空隙数目，发生碰撞的空隙数目和成功识别标签的空隙数目的数量估计当前的标签数并设置下一帧的最优的长度；另一种根据前一时隙的反馈动态调整帧长为2的整数倍，这种方法最具代表性的是EPCglobal Gen2标准中设计的Q算法。



基于二进制树的防冲突算法

查询二进制树

查询二进制树算法是无状态协议，不需标签内部维持任何状态，标签只需根据阅读器广播的标识符前缀作比较即可。



阅读器内部维持一个二进制前缀，初始值为0。每一个时隙开始时，阅读器广播该二进制前缀，电子标签将自己的标识符号前几位与此二进制前缀进行比较，若相同则立即发送标识符号。

如果阅读器探测到冲突发生，则在下次查询中在原来的二进制前缀后面增加0或1，重新查询，如此循环直到识别完所有的标签。



本章内容

- 2.1 自动识别技术
- 2.2 RFID的历史和现状
- 2.3 RFID技术分析
- 2.4 RFID标签冲突*
- 2.5 **RFID和物联网**

基于RFID标签对物体唯一标识特性引发了对物联网研究的热潮。





2.5 RFID与物联网

基于RFID标签对物体的唯一标识特性，引发了人们对实物互联网（物联网）研究的热潮。

物联网是通过给所有物品贴上RFID标签，在现有互联网基础之上构建所有参与流通的物品信息网络。

物联网的建立将对生产制造、销售、运输、使用、回收等物品流通的各个环节以及政府、企业和个人行为带来深刻影响。

通过物联网，世界上任何物品都可以随时随地按需被标识、追踪和监控。

物联网被视为继Internet后IT业的又一次革命。



本章小结

内容回顾

- 本章对常见的自动识别方法和技术做了介绍，包括：光学符号识别技术、语音识别技术、生物计量识别技术、IC卡技术、条形码技术和RFID射频技术
- 本章重点讲述了RFID技术，包括RFID历史和现状、RFID技术剖析和RFID标签冲突问题。



本章小结

重点掌握

- 光学符号识别技术的基本概念，语音识别的流程，虹膜识别的特点，指纹的整体特征和局部特征。
- IC卡系统的构成及分类方法。
- 条形码的分类，一维条形码的组成，条形码模块的概念；一维条形码的基本参数及工作原理，二维条形码与一维条形码的比较，常见的一维条形码和二维条形码编码。



本章小结

重点掌握（续）

- RFID的概念与现状。
- RFID系统的组成，RFID标签的优点和特点，RFID标签的存储方式及分类，RFID系统的常见频率及其优缺点。
- RFID标签冲突及防冲突算法的概念，防冲突算法分类，详细描述基于帧的分时隙的ALOHA协议，Q协议、随机二进制树协议和查询二叉树协议。以上各种协议的优缺点。

GreenOrbs
Pervasive Computing
to IoT
of
OceanSense
Smart Planet
Smart Grid
Introduction
Things

zigBee Web ITU BlueTooth
nesC ETC
PDA IPv6 RFID Database
TinyOS ITS
CPS
CDMA SQL



Thank you!



Internet of Things