



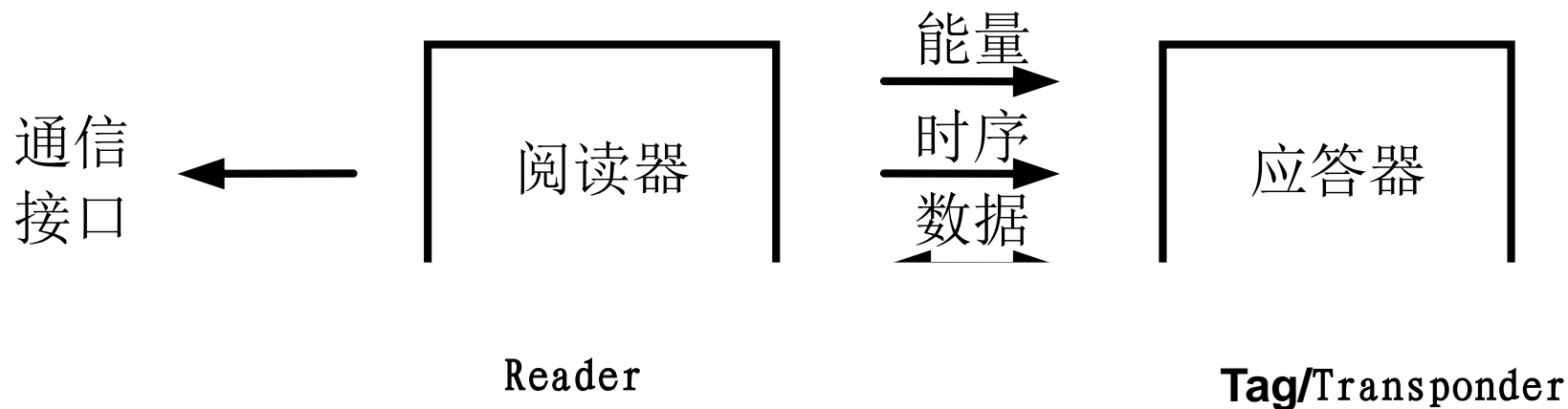
# RFID复习

# 一、RFID概论

- 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。
- **Radio frequency identification**
- RFID系统中，识别信息存放在电子数据载体中，电子数据载体称为应答器。
- 应答器中存放的识别信息由阅读器读出。
- 阅读器不仅可以读出存放的信息，而且可以对其进行写入，读写过程是通过双方之间的无线通信来实现的。

# 一、RFID概论

RFID的基本原理框图

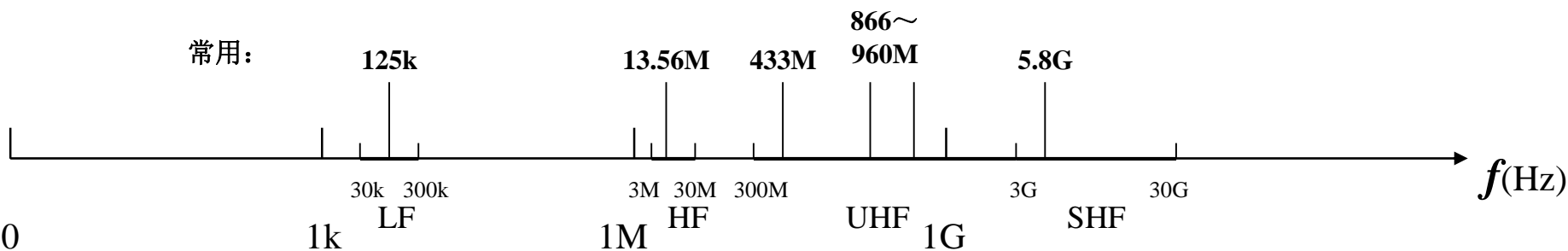


射频识别系统的

**原理 构成 各部分作用 各部分包含的功能**

# 一、RFID概论

## ■ RFID的工作频率分类



### 按工作频率分

低频

125Khz

小于10cm

高频

13.56Mhz

10cm

超/特高频

上百兆hz

微波

GHz

数米

传输  
距离  
越来越远

## I 低频 Low Frequency(LF): 主要规格125~134KHz。

低频的最大优点在于其标签靠近金属或液体的物品能够有效发射讯号，不像其他较高频率标签的讯号会被金属或液体反射回来，但缺点是读取距离短、无法同时进行多标签读取以及资讯量较低，一般应用于门禁系统、动物晶片、汽车防盗器和玩具等。

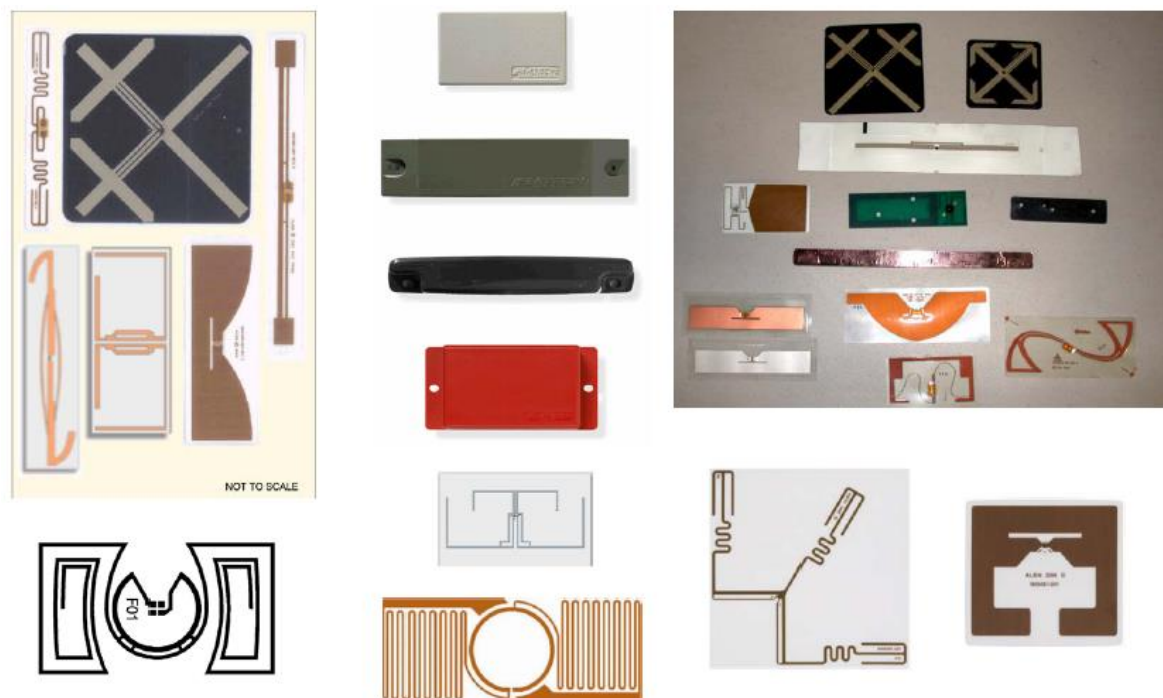


## II 高频 High Frequency(HF): 主要规格13.56MHz 。

- 常见的主要规格有13.56MHz;
- ISO-14443A Mifare和 ISO-15693;
- 电子卷标都是被动式感应耦合, 读取距离约10-100公分;
- 优点在于传输速度较快且可进行多标签辨识;
- 缺点是环境干扰较为敏感, 在金属或较潮湿的环境下, 读取率较低;
- 应用于门禁系统、悠游卡、电子钱包、图书管理、产品管理、文件管理、栈板追踪、电子机票、行李卷标;
- 技术最成熟且应用和市场也最广泛且接受度高;
- 故建议现阶段应大力发展此领域技术和应用。

## II 超高频Ultra High Frequency(UHF): 主要规格

433MHz、860MHz~960MHz。



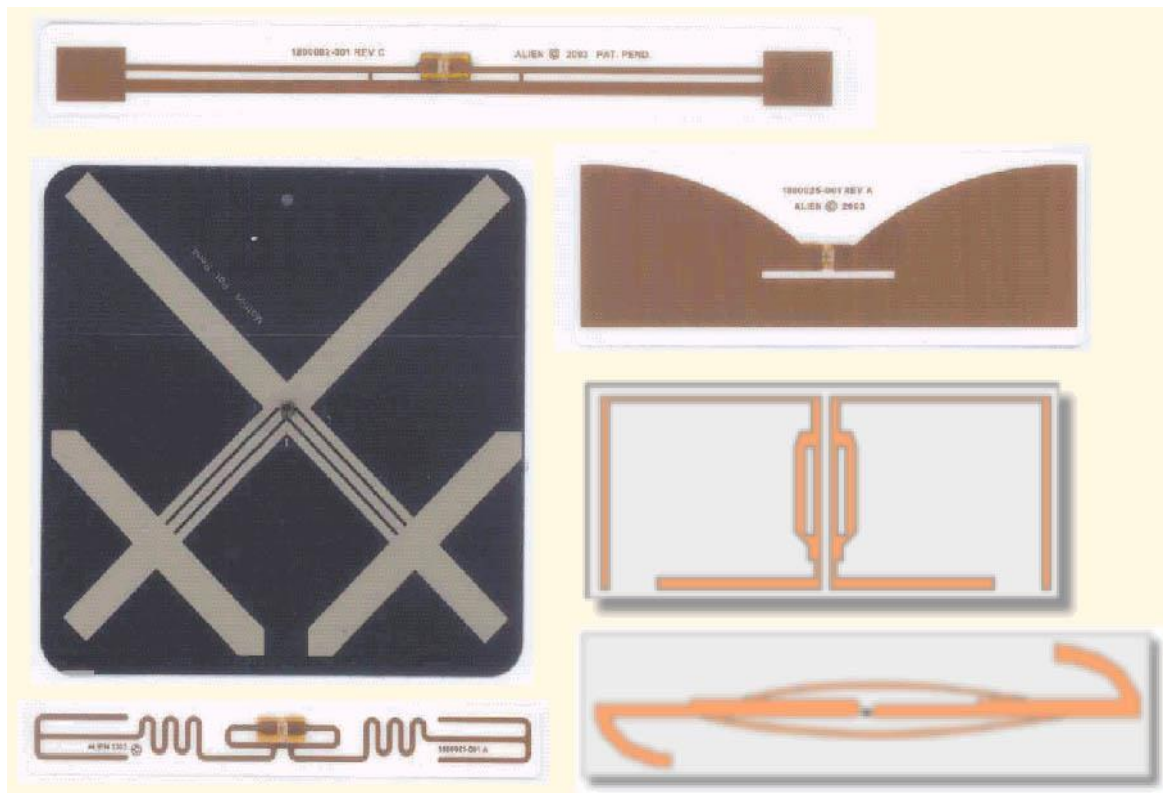
虽然在金属与液体的物品上应用较不理想，但由于读取距离较远、资讯传输速率较快，而且可以同时进行大量标签的读取与辨识，因此目前已成为市场主流，未来将广泛应用于航空旅客与行李管理系统、货架及栈板管理、出货管理、物流管理...等

(图1-27超高频电子标签)。

### III 极高频/微波Super High

Frequency(SHF)/Microwave(uW): 主要规格**2.4GHz**、**5.8GHz**

特性与应用和超高频段相似，但是对于环境的敏感性较高，像是易被水气吸收，实作较复杂，未完全标准化，普及率待观察，一般应用于行李追踪、物品管理、供应链管理...等。





按电源分

有源

无源

半有源

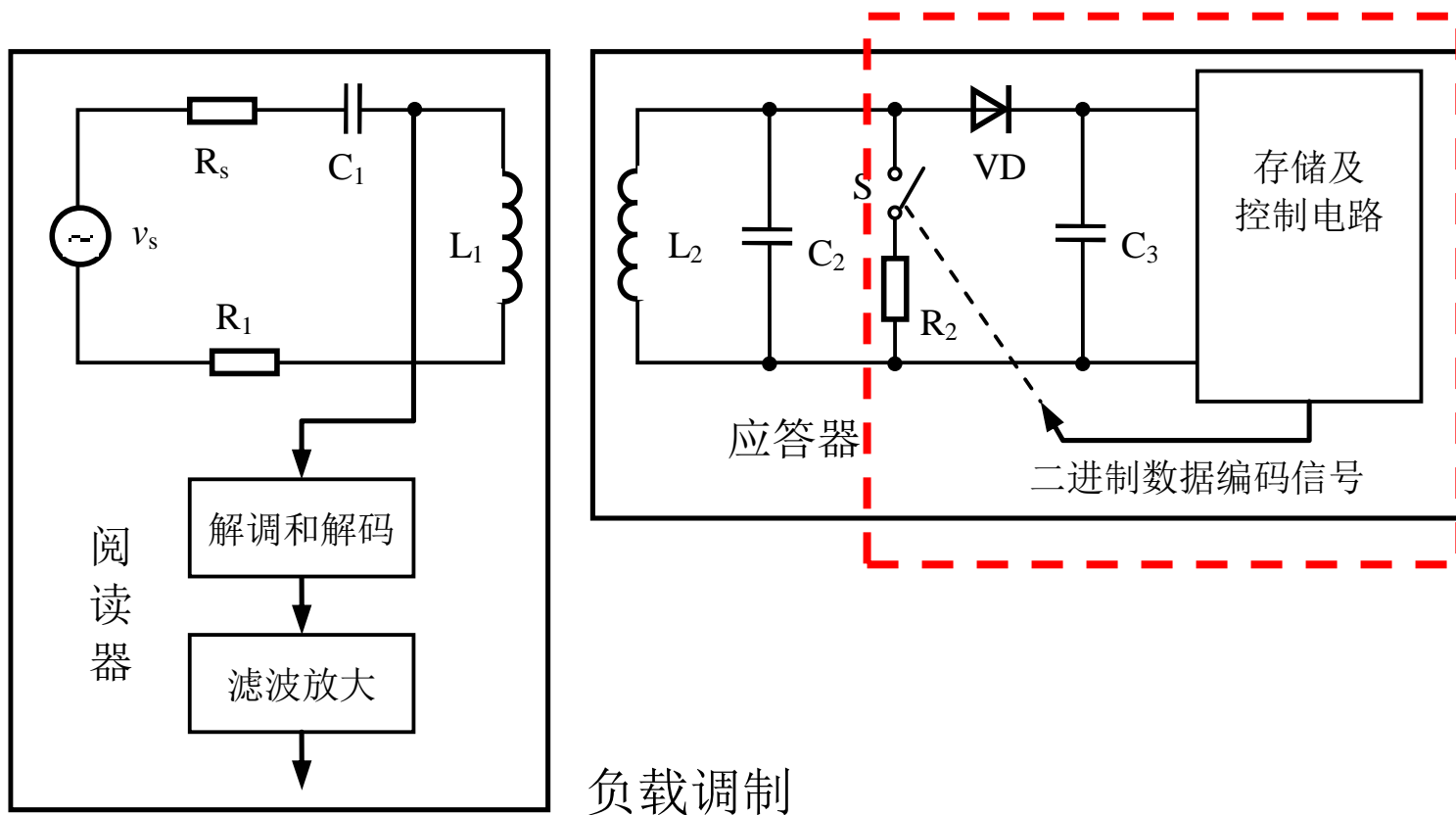
## ■ 无源、半无源与有源应答器

- **无源应答器：** 不附有电池，从阅读器发出射频能量中提取工作所需的电能。采用电感耦合方式的应答器多为无源应答器。
- **半无源应答器：** 内装有电池，起辅助作用，对维持数据的电路供电或对应答器芯片工作所需的电压作辅助支持，用于传输通信的射频能量源自阅读器。
- **有源应答器：** 工作电源完全由内部电池供给，同时内部电池能量也部分地转换为应答器与阅读器通信所需的射频能量。

# 一、RFID概论

## ■ RFID工作方式

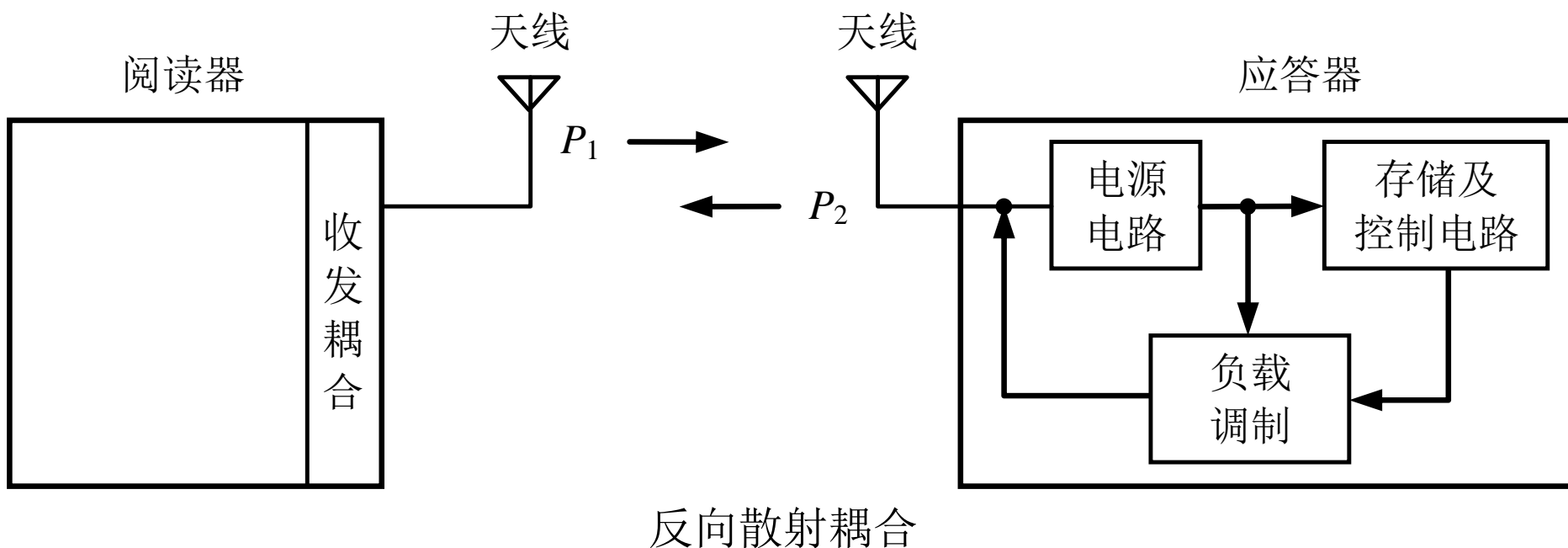
## 1.电感耦合式 最常用



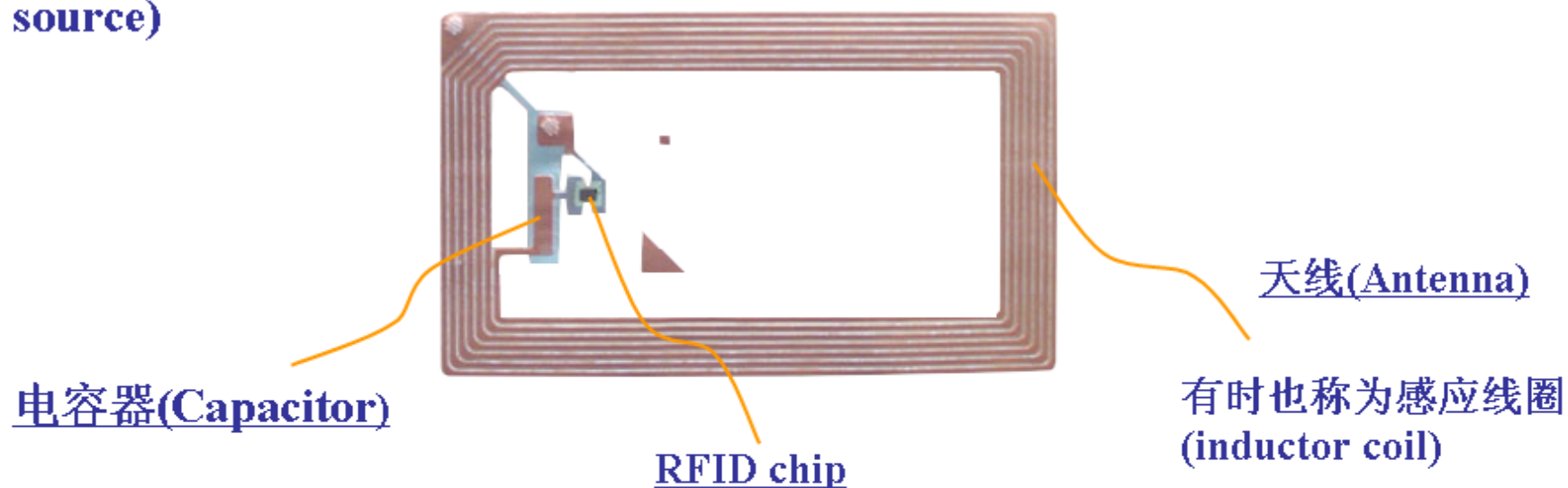
# 一、RFID概论

## ■ RFID工作方式

### 1.反向散射式



一个RFID Tag的组成包含：RFID chip、天线(antenna)及电力来源(Power source)



亦称 Application Specific Integrated Circuit (ASIC)

RFID chip组成包含有：

调变电路(modulation circuitry)

控制电路(control circuitry)

记忆体( memory)

处理器(processor)

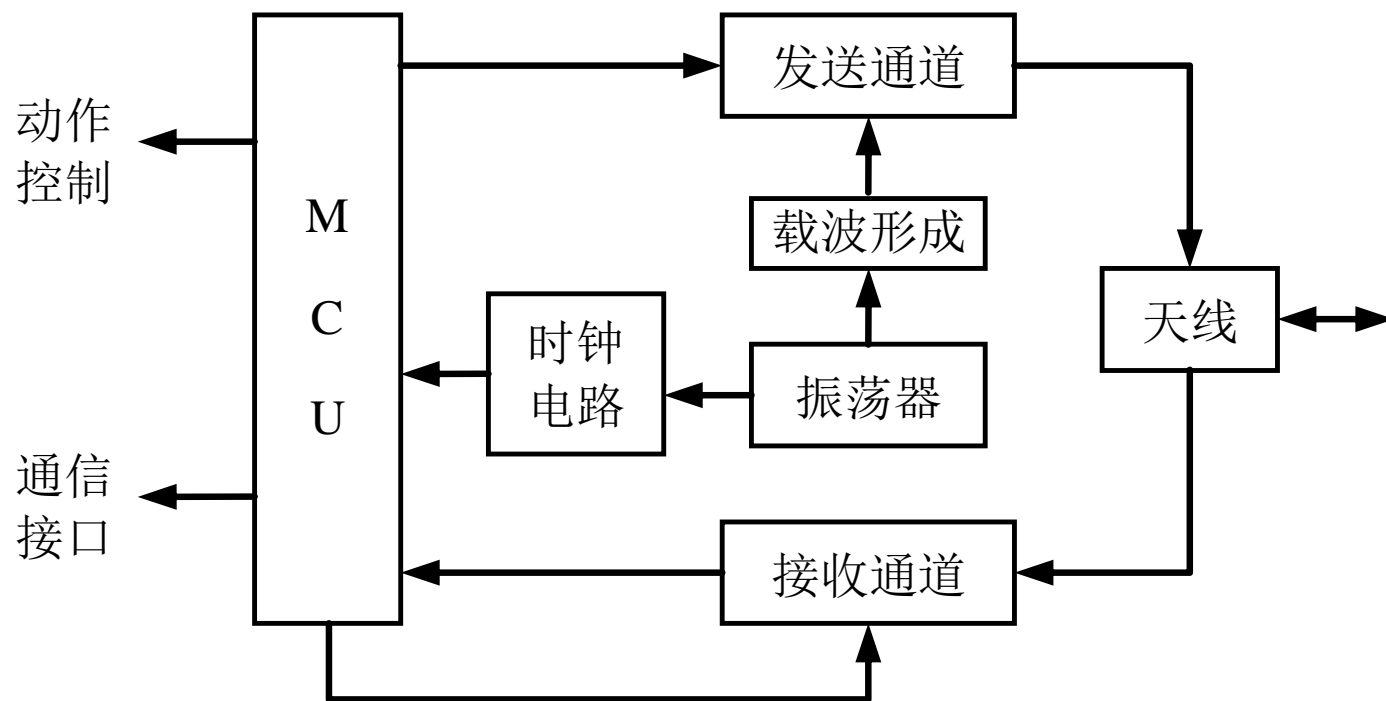
# 一、RFID概论

## ■ 阅读器的功能

- ① 以射频方式向应答器传输能量;
- ② 从应答器中读出数据或向应答器写入数据;
- ③ 完成对读取数据的信息处理并实现应用操作;
- ④ 若有需要, 应能和高层处理交互信息。

# 一、RFID概论

## ■ 阅读器的电路组成



# 一、RFID概论

## ■ 天线

- 天线的目标是取得最大的能量传输效果。
- **RFID**系统所用的天线类型主要有偶极子天线、微带贴片天线、线圈天线等。
- 在应答器中，天线和应答器芯片封装在一起。

# 一、RFID概论

## ■ RFID的应用举例

- RFID应用领域广泛，且每种应用的实现，都会形成一个庞大的市场，因此可以说射频识别是一个重要的新的经济增长点。
- 目前，RFID在票务系统（城市公交车、高速公路收费、门票等）、收费卡、城市交通管理、安检门禁、物流、家政、食品安全追溯、药品、矿井生产安全、防盗、防伪、证件、集装箱识别、动物追踪、运动计时、生产自动化、商业供应链等众多领域获得广泛重视和应用。



- 
- RFID及其相关识别技术（P14）
  - 类型
  - 特点（rfid最大特点非接触式）

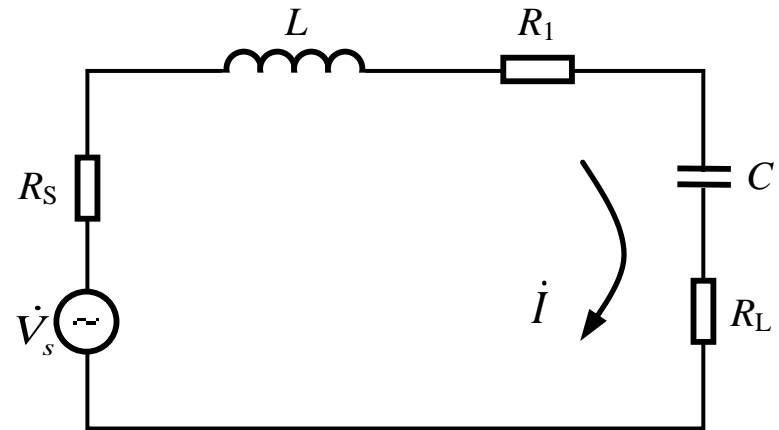
## 2 电感耦合方式的射频前端

### ■ 串联谐振回路

回路电流  $\dot{I}$

$$\dot{I} = \frac{\dot{V}_s}{Z} = \frac{\dot{V}_s}{R + jX} = \frac{\dot{V}_s}{R + j\left(\omega L - \frac{1}{\omega C}\right)}$$

阻抗  $|Z| = \sqrt{R^2 + X^2} = \sqrt{R^2 + \left(\omega L - \frac{1}{\omega C}\right)^2}$  相角  $\varphi = \arctan \frac{X}{R} = \arctan \frac{\omega L - \frac{1}{\omega C}}{R}$



## 2 电感耦合方式的射频前端

### ■ 串联谐振回路

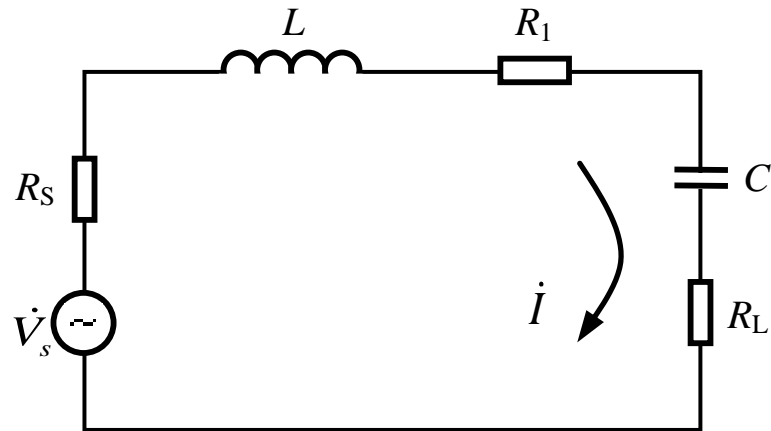
串联回路的谐振条件

$$X = \omega L - \frac{1}{\omega C} = 0$$

谐振频率

$$\omega_0 = \frac{1}{\sqrt{LC}}$$

$$f_0 = \frac{1}{2\pi\sqrt{LC}}$$

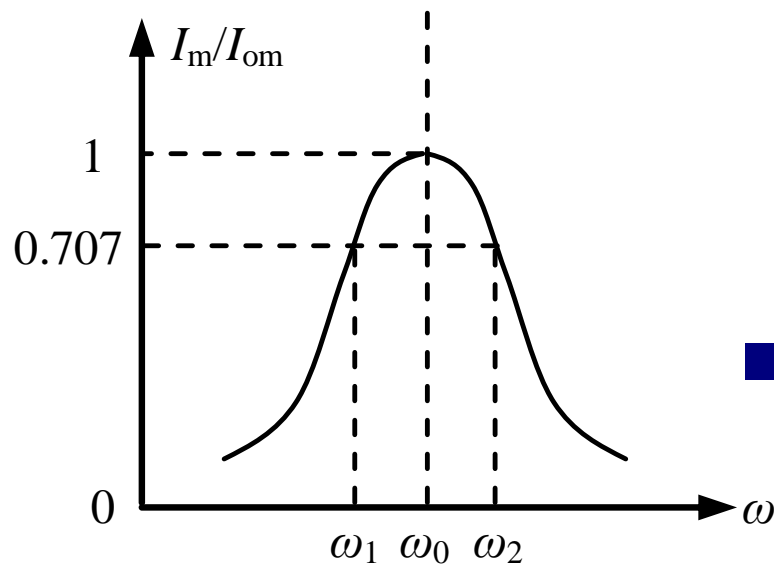


$$\omega_0 L = \frac{1}{\omega_0 C} = \sqrt{\frac{L}{C}} = \rho$$

## 2 电感耦合方式的射频前端

### ■ 通频带

谐振回路的通频带通常用半功率点的两个边界频率之间的间隔表示，半功率的电流比 $I_m/I_{0m}$ 为0.707



通频带

### ■ 品质因素

$$Q = \frac{\omega L}{R} = \frac{1}{\omega CR}$$

$$BW = \frac{\omega_2 - \omega_1}{2\pi} = \frac{2(\omega_2 - \omega_0)}{2\pi} = \frac{2\Delta\omega_{0.7}}{2\pi} = \frac{\omega_0}{2\pi Q} = \frac{f_0}{Q}$$

## 2 电感耦合方式的射频前端

- 串联谐振 并联谐振比较
- 电路连接方式
- 谐振时的L和C上的电压电流大小

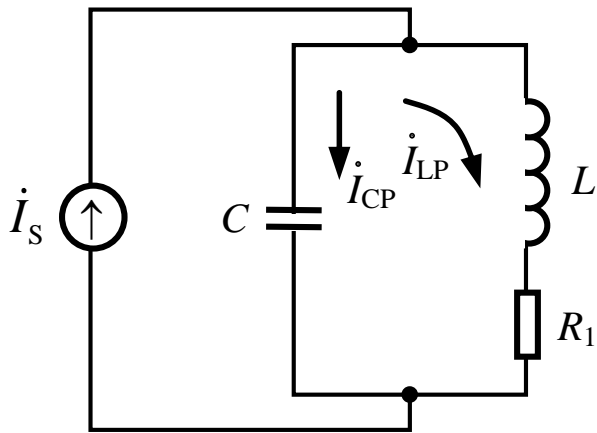
## 2 电感耦合方式的射频前端

- 电阻负载调制
- 电容负载调制
- 原理 与构成

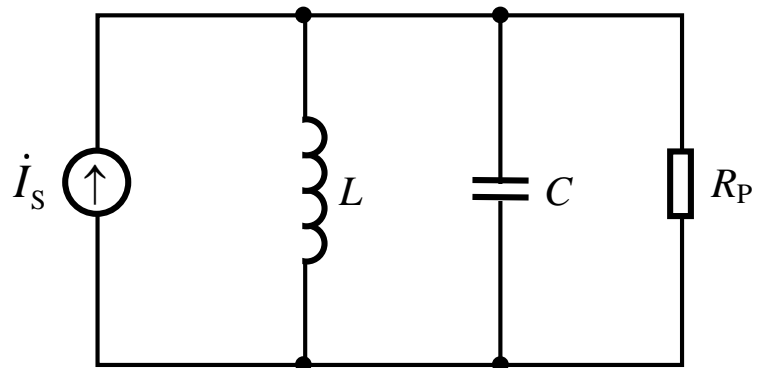
## 2 电感耦合方式的射频前端

### ■ 并联谐振回路

- 串联谐振回路适用于恒压源，即信号源内阻很小的情况。
- 如果信号源的内阻大，应采用并联谐振回路。
- 在研究并联谐振回路时，采用恒流源（信号源内阻很大）分析比较方便。

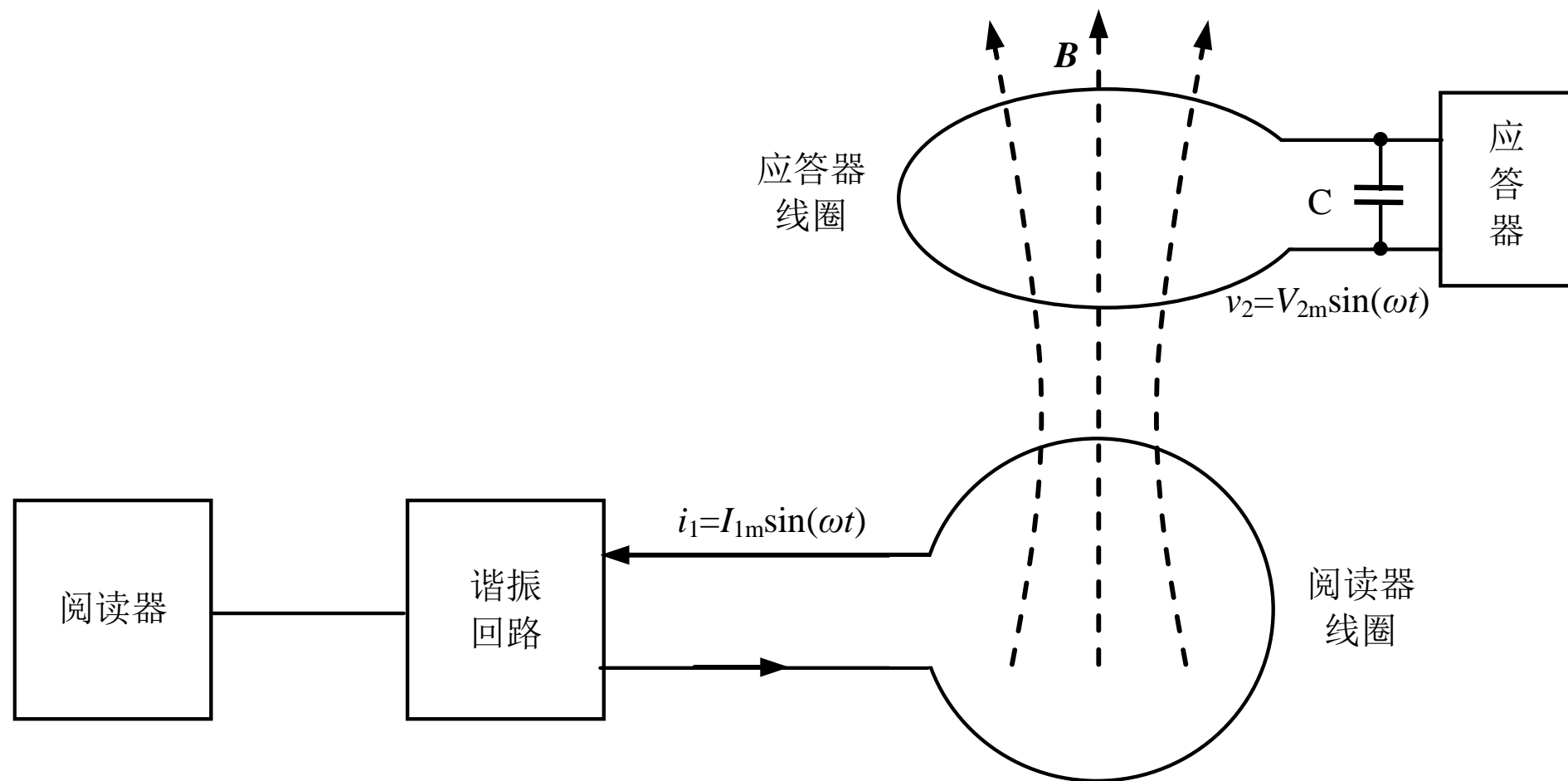


(a) 损耗电阻和电感串联



(b) 损耗电阻和回路并联

## 2 电感耦合方式的射频前端

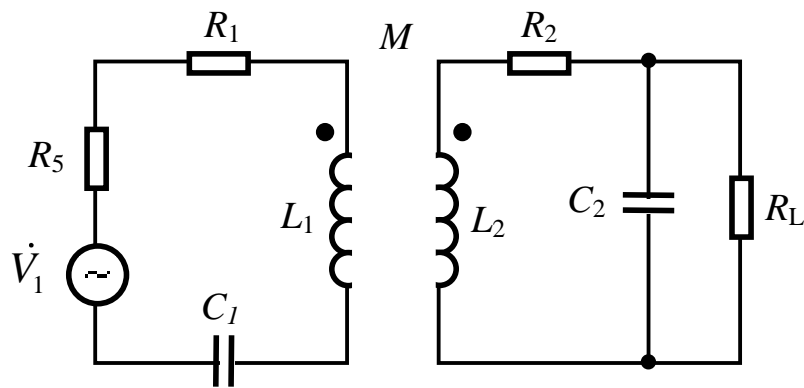




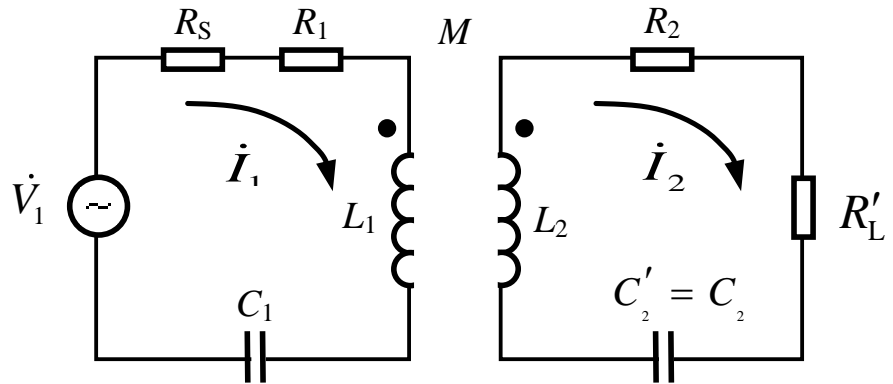
## 2 电感耦合方式的射频前端

### ■ 负载调制

□ 应答器向阅读器的信息传送时采用



(a) 耦合电路

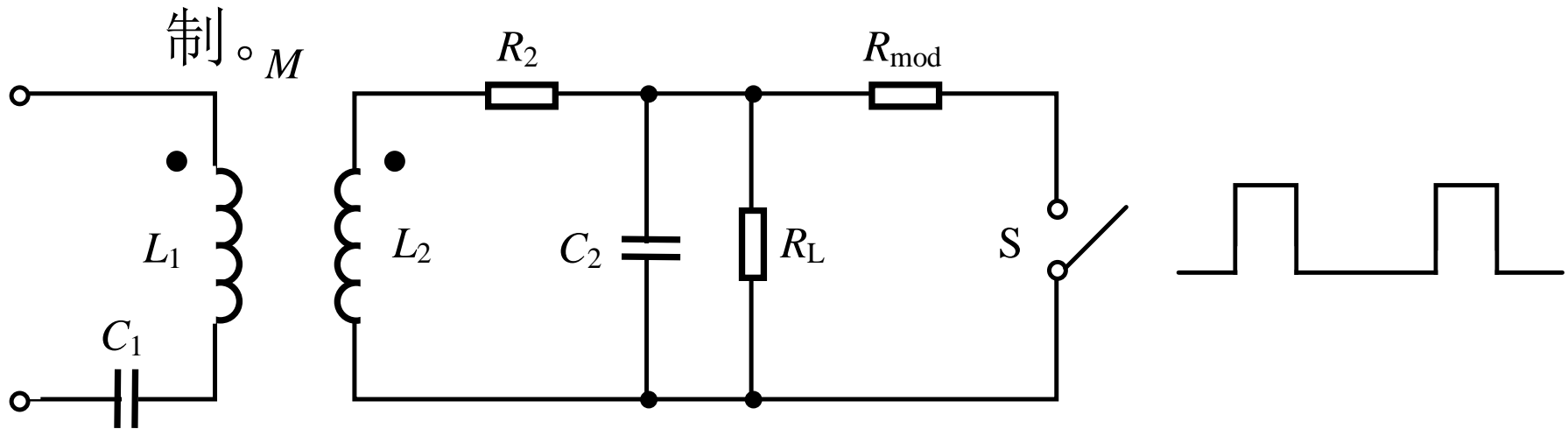


(b) 次级经过等效变换后的耦合电路

## 2 电感耦合方式的射频前端

### ■ 电阻负载调制

- 开关S用于控制负载调制电阻 $R_{\text{mod}}$ 的接入与否，开关S的通断由二进制数据编码信号控制。



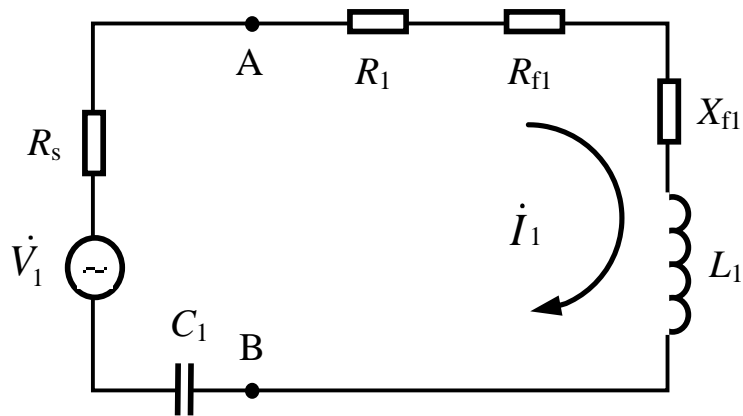
## 2 电感耦合方式的射频前端

### ■ 电阻负载调制

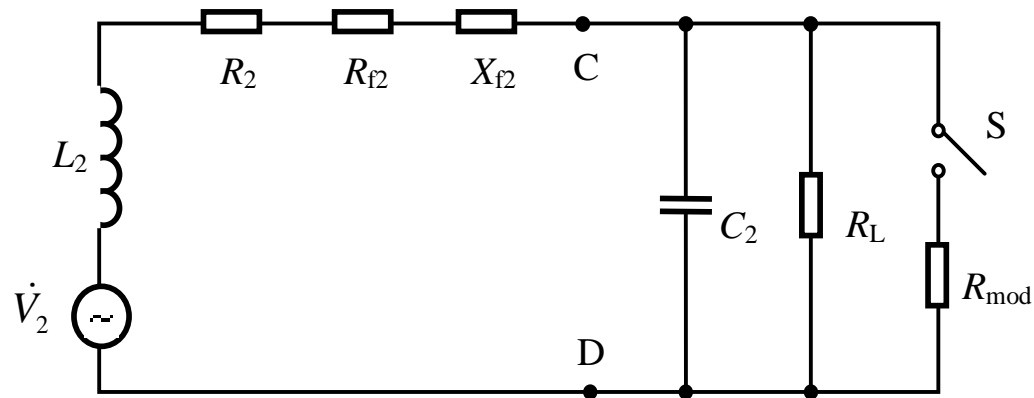
- 二进制数据编码信号用于控制开关 $S$ 。当二进制数据编码信号为“1”时，设开关 $S$ 闭合，则此时应答器负载电阻为 $R_L$ 和 $R_{mod}$ 并联；而二进制数据编码信号为“0”时，开关 $S$ 断开，应答器负载电阻为 $R_L$ 。
- 应答器的负载电阻值有两个对应值，即 $R_L$ （ $S$ 断开时）和 $R_L$ 与 $R_{mod}$ 的并联值 $R_L // R_{mod}$ （ $S$ 闭合时）。

## 2 电感耦合方式的射频前端

### ■ 电阻负载调制



(a) 初级回路等效电路



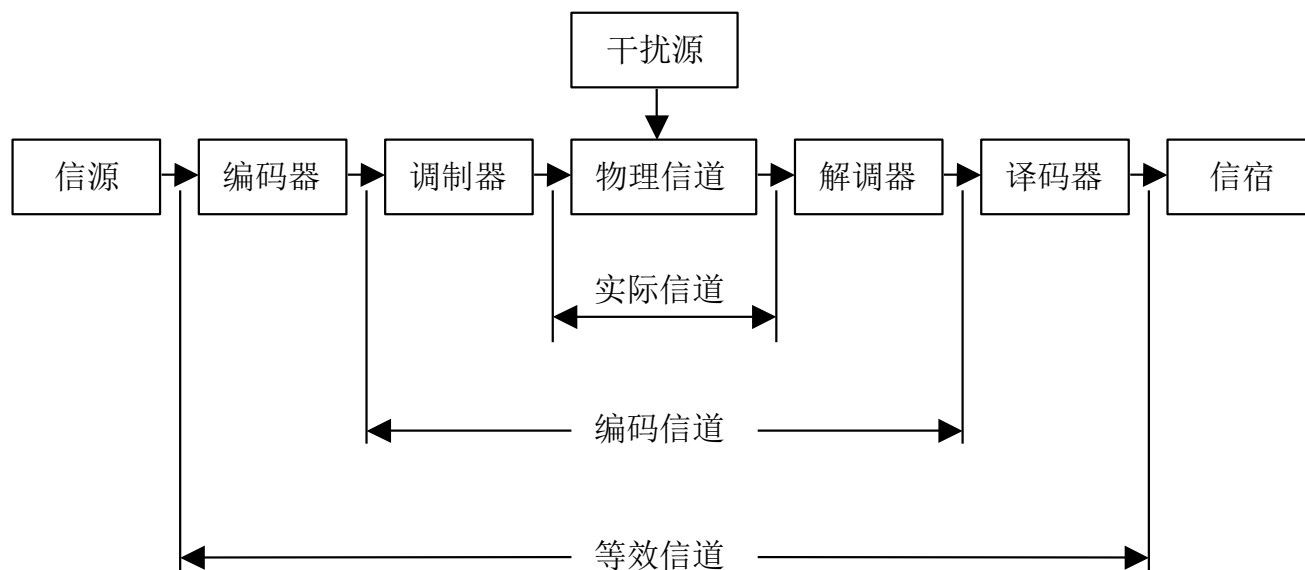
(b) 次级回路等效电路

次级回路等效电路中的端电压

$$\dot{V}_{CD} = \frac{\dot{V}_2}{1 + [(R_2 + R_{f2}) + j\omega L_2] \left( j\omega C_2 + \frac{1}{R_{Lm}} \right)}$$

- 
- 功率放大器的效率比较
  - B类小于D类

# 信道



数字通信系统的一般模型

# 传输损耗与失真

- 衰减效应
- 延迟变形 时延
- 多径效应

# 波特率与比特率

## ■ 比特率：

比特率是指每秒传送的比特(bit)数。单位为 **bps(Bit Per Second)**，比特率越高，传送数据速度越快。每秒钟通过信道传输的信息量称为位传输速率，也就是每秒钟传送的二进制位数，简称比特率。比特率表示有效数据的传输速率。

## ■ 波特率：

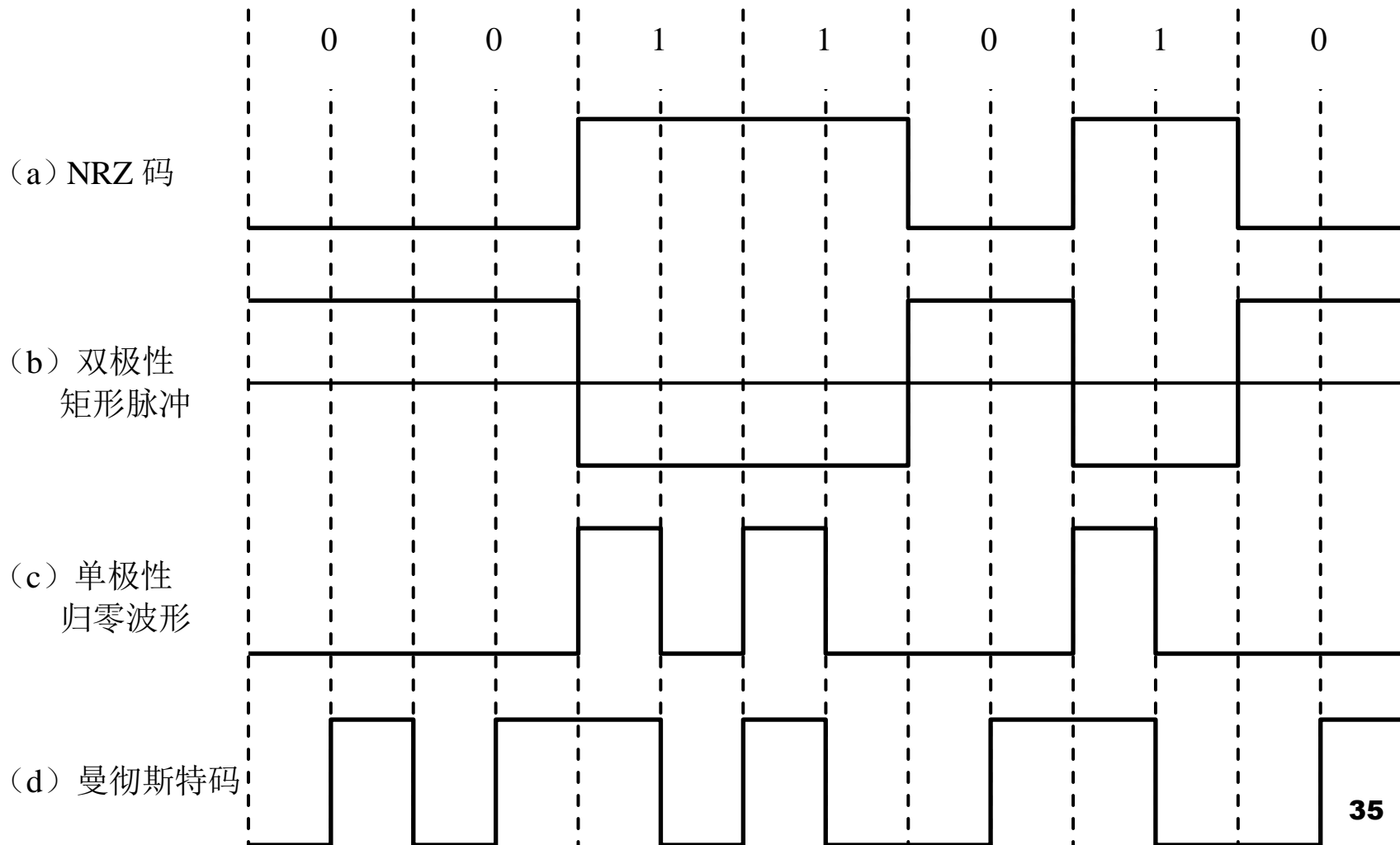
在信息传输通道中，携带数据信息的信号单元叫码元，每秒钟通过信道传输的码元数称为码元传输速率，简称波特率。波特率是指数据信号对载波的调制速率，它用单位时间内载波调制状态改变的次数来表示(也就是每秒调制的符号数)，其单位是波特 (**Baud, symbol/s**)。波特率是传输通道频宽的指标。



- 波特率与比特率的关系：  
比特率=波特率 $\times$ 单个调制状态对应的二进制位数。
- 例如：假设数据传送速率为120符号/秒(也就是波特率为120Baud)，又假设每一个符号为8，即八相调制(单个调制状态对应3个二进制位)，则其传送的比特率为(120symbol/s)  $\times$  (3bit/symbol)=360bps。

# 3 编码和调制

## ■ 数字基带信号波形



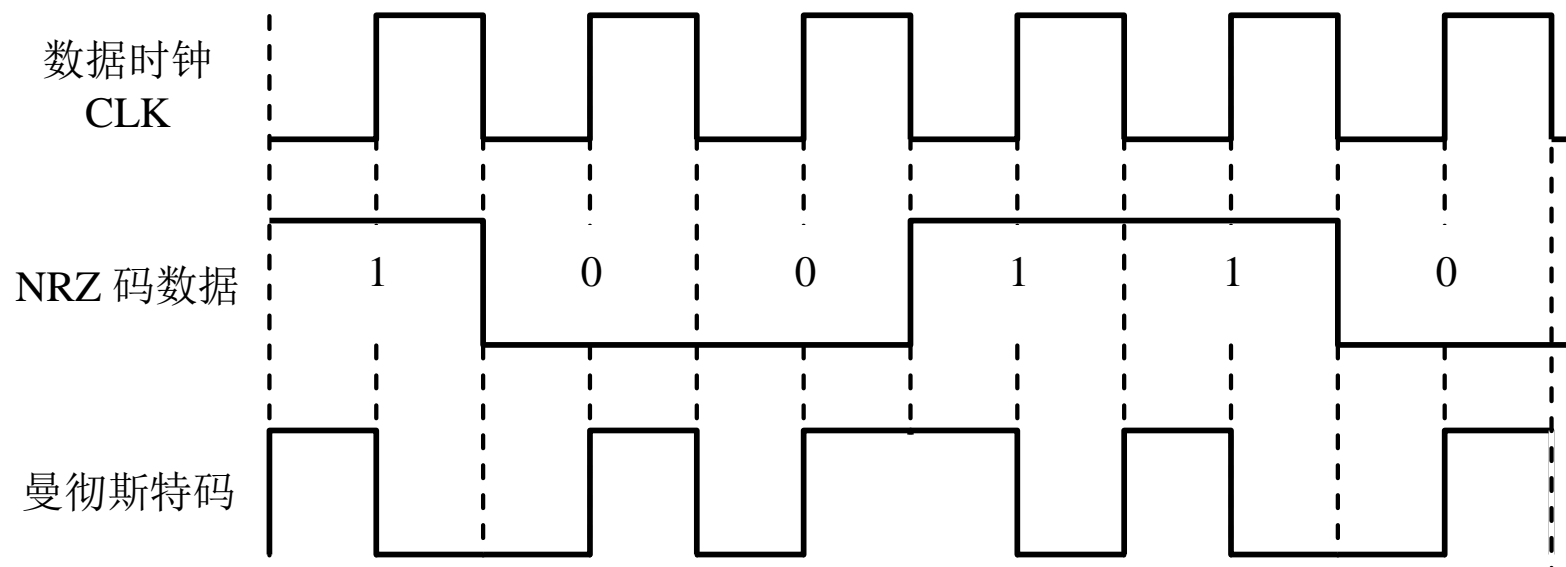


■ 射频识别系统通常使用下列编码方法中的一种：

- 反向不归零（**NRZ**）编码
- 曼彻斯特（**Manchester**）编码
- 单极性归零（**UnipolarHZ**）编码
- 密勒（**Miller**）编码。

# 3 编码和调制

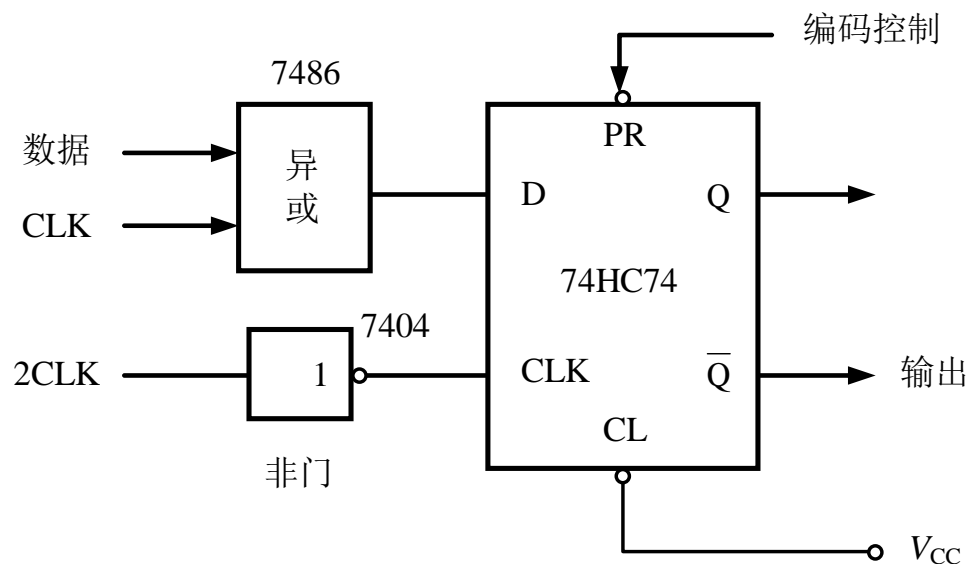
- RFID中常用的编码方式及编解码器
- 曼彻斯特（Manchester）码



■ 10 表示数据1

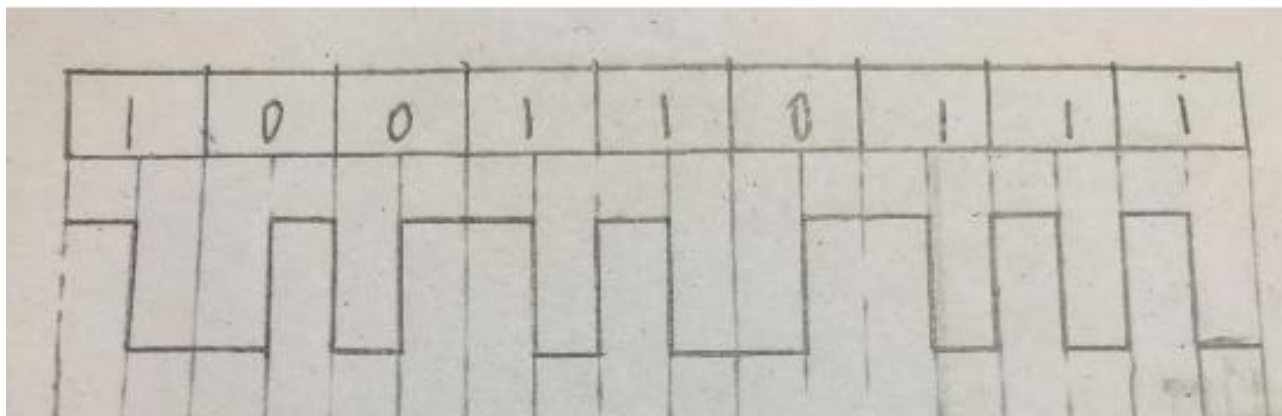
■ 01 表示数据0

## ■ 曼彻斯特（Manchester）码

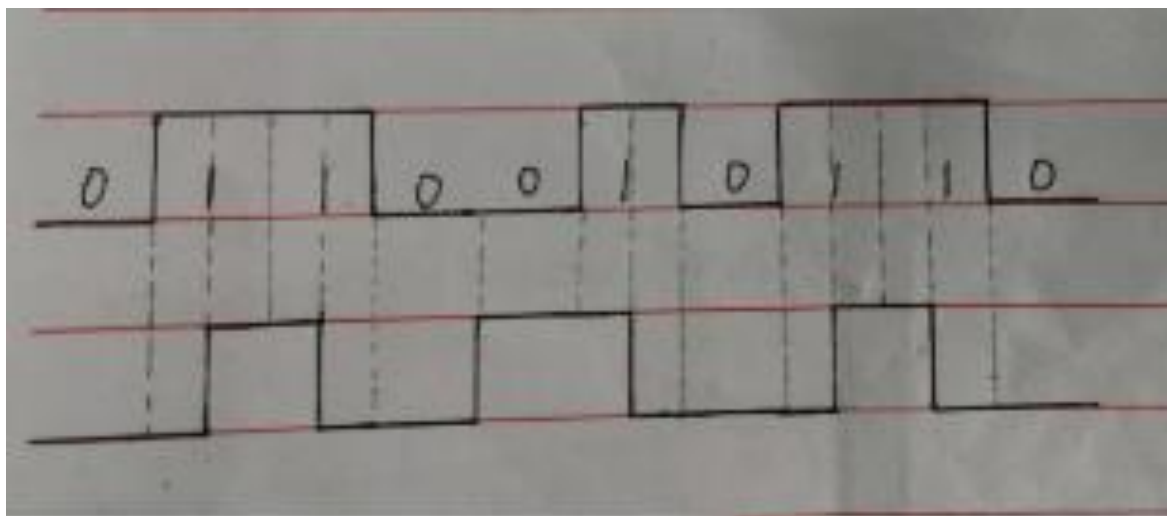


**编码器电路**  
**从NRZ码到曼彻斯特码**

## ■ 曼彻斯特（Manchester）码



## ■ 密勒码



# 3 编码和调制

## ■RFID中常用的编码方式及编解码器

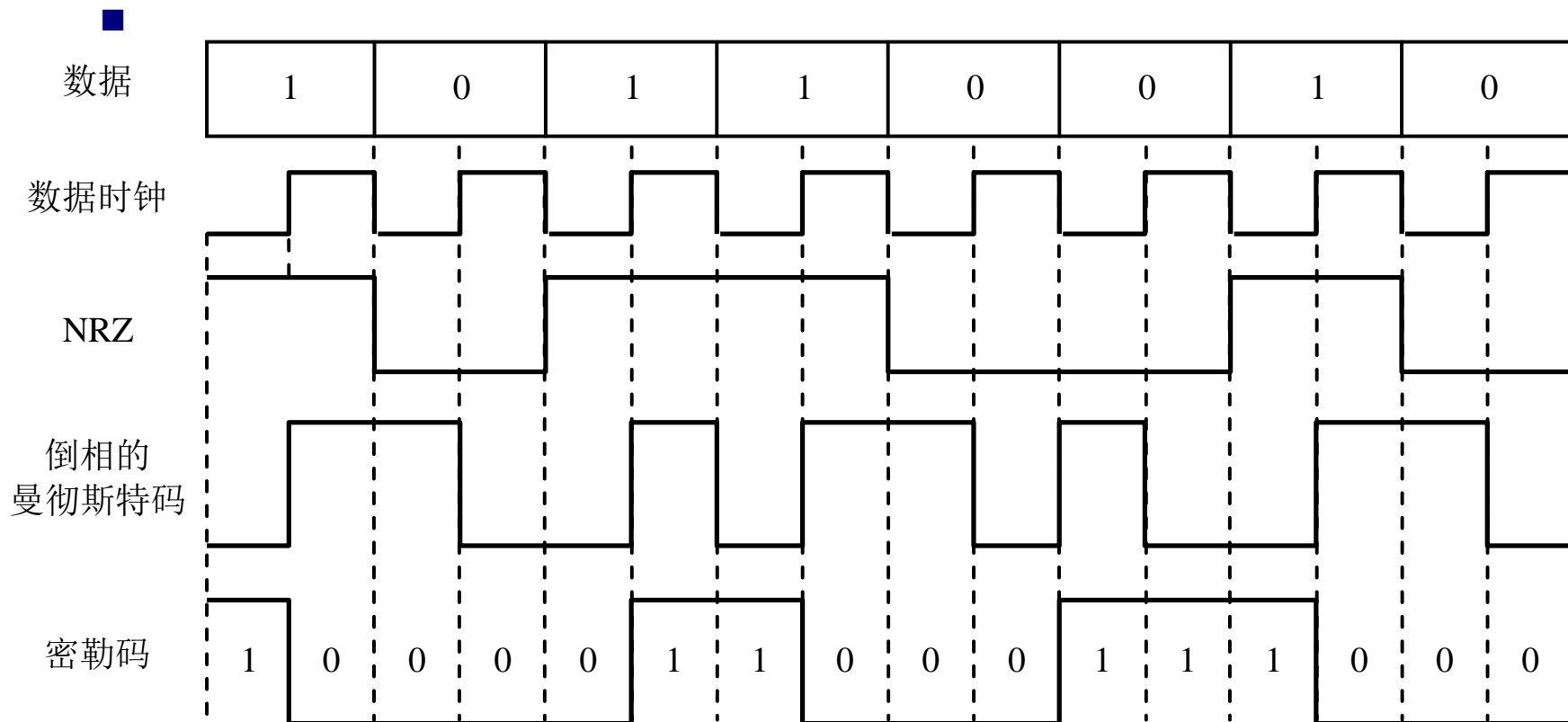
### ■ 密勒（Miller）码

密勒码编码规则

bit(i-1)	bit i	密勒码编码规则
×	1	bit i的起始位置不变化，中间位置跳变
0	0	bit i的起始位置跳变，中间位置不跳变
1	0	bit i的起始位置不跳变，中间位置不跳变

# 3 编码和调制

## ■RFID中常用的编码方式及编解码器



密勒码波形及与NRZ码、曼彻斯特码的波形关系



# 3 编码和调制

- 脉冲调制

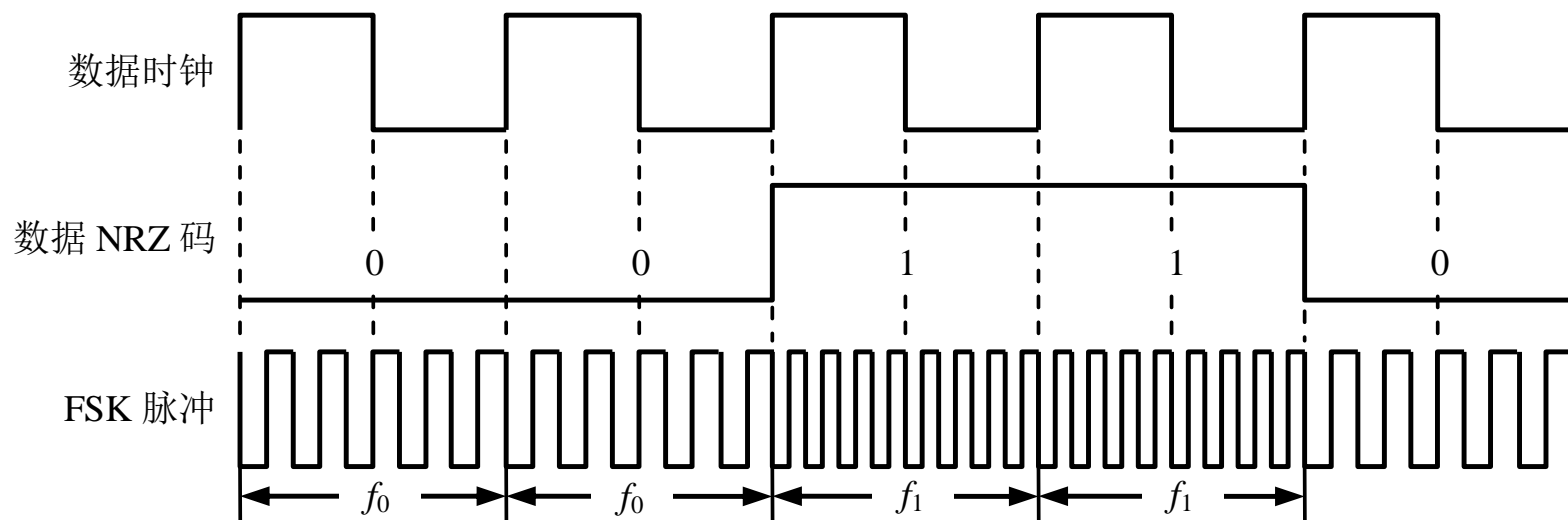
- 将数据的NRZ码变换为更高频率的脉冲串，该脉冲串的脉冲波形参数受NRZ码的值0和1调制。

- 主要的调制方式为频移键控FSK和相移键控PSK。

# 3 编码和调制

## ■ 脉冲调制

## ■ FSK



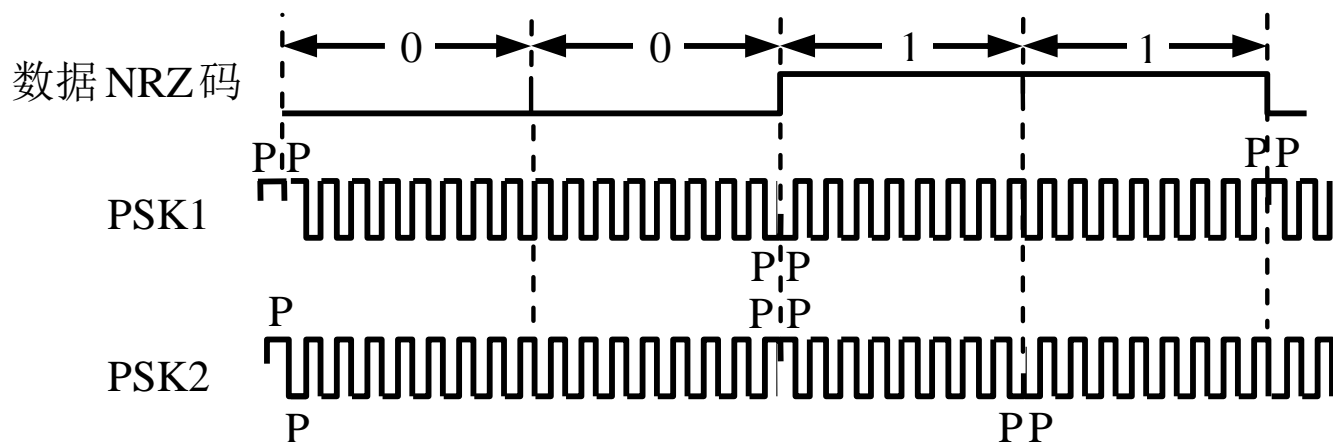
FSK脉冲调制波形

FSK是指对已调脉冲波形的频率进行控制，  
FSK调制方式用于射频载波频率为125kHz的情况。

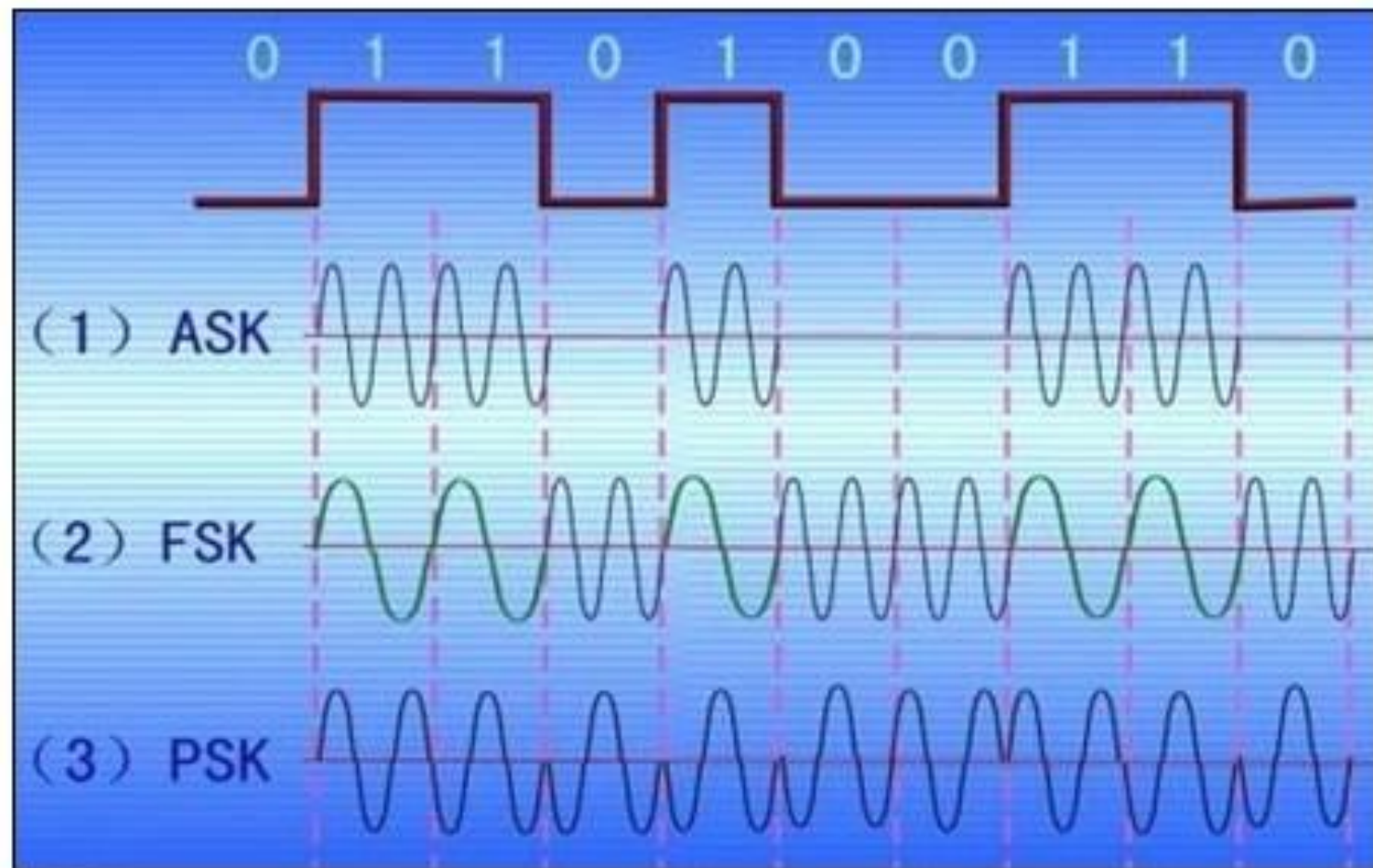
# 3 编码和调制

## ■ 脉冲调制

## ■ PSK1和PSK2

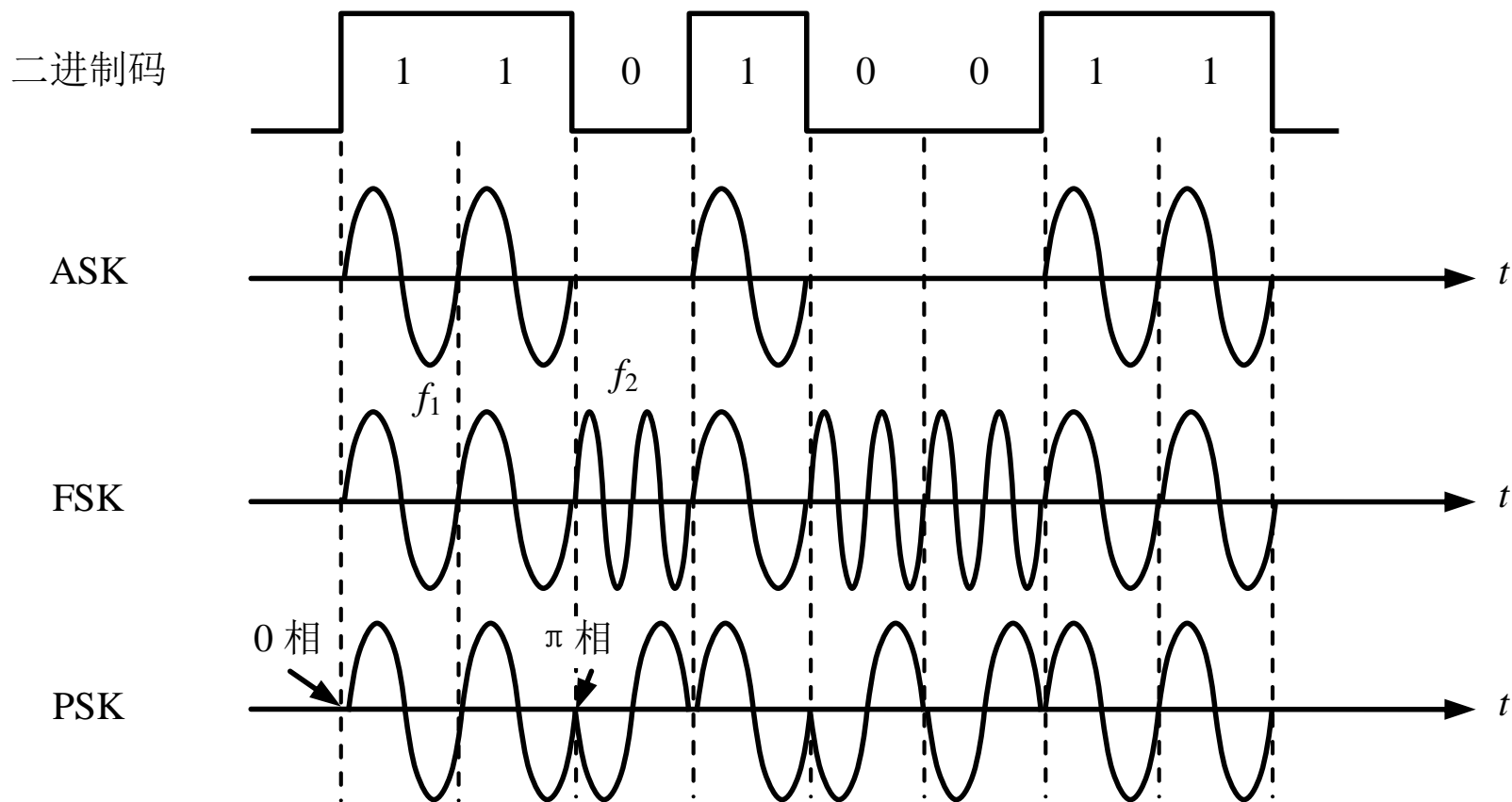



采用PSK1调制时，若在数据位的起始处出现上升沿或下降沿（即出现1，0或0，1交替），则相位将于位起始处跳变 $180^\circ$ 。而PSK2调制时，相位在数据位为1时从位起始处跳变 $180^\circ$ ，在数据位为0时则相位不变。



说明三种调制方式的特点

### 3 编码和调制






在RFID系统中，数据传输的完整性存在两个方面的问题：

- 外界的各种干扰可能使数据传输产生错误；
- 多个应答器同时占用信道使发送数据产生碰撞。

运用数据检验（差错检测）和 防碰撞算法可分别解决这两个问题。



# 数据校验

# 0、差错原因

## ● 信道噪声

### ☞ 热噪声

- ❖ 由**传输媒体**的电子热运动引起
- ❖ 时刻存在，幅度小，属于**随机噪声**

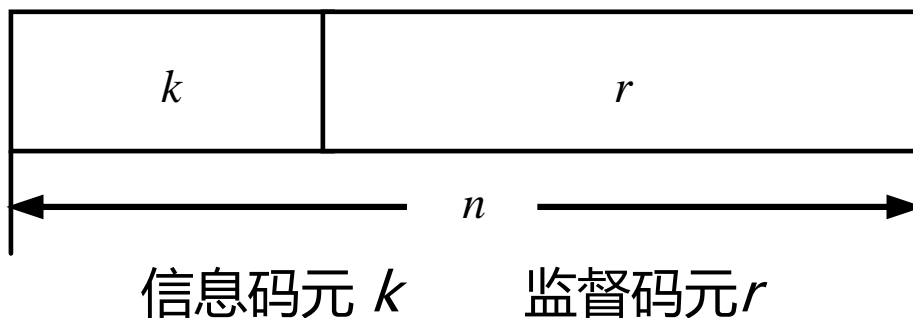
### ☞ 冲击噪声

- ❖ 是由外界**电磁**干扰引起
- ❖ 幅度较大，是引起**差错**的主要原因
- ❖ 冲击噪声引起的传输差错称为**突发差错**



## 4.1.3 检纠错码

### □ 信息码元与监督码元



总码元数为  $n = k + r$ ;  $(n, k)$  码

• 编码效率  $k/n$

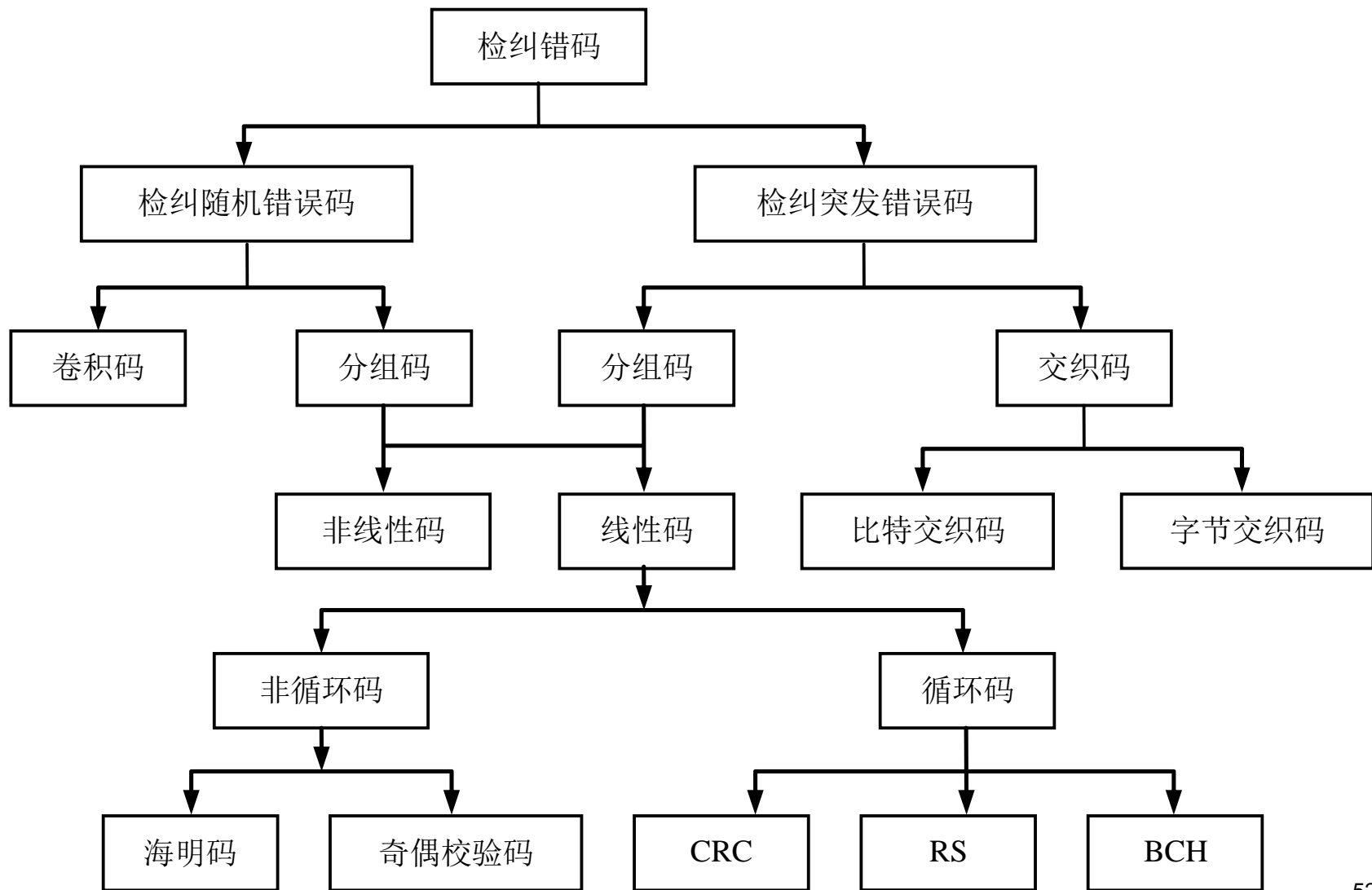
许用码组	$2^k$
禁用码组	$2^n - 2^k$

## 汉明距离

汉明距离（码距）是指每两个码组间的距离。即两码组对应位取值不同的个数（**异或后1的个数**）。

例如：**000**和**111**之间的汉明距离为**3**。

## 检纠错码的分类



## ■ 分组码

- 码组的监督码元仅与本码组的信息码元有关，而与其他码元组的信息码元无关

## ■ 卷积码

- 码组的监督码元不仅与本码组的信息码元相关，而且与本码组相邻的前 $m$ 个时刻输入的码组的信息码元之间也具有约束关系
- 性能优于分组码

## ■ 交织码

- 利用交织技术构造出来的编码 (二维矩阵)

## 差错控制

- 在传输信息数据中增加一些冗余编码，使监督码元和信息码元之间建立一种确定的关系，实现差错控制编码和差错控制解码功能。
- 反馈重发（ARQ）、前向纠错（FEC）和混合纠错（HEC）
  - 反馈重发发送端需要在得到接收端正确收到所发信息码元（通常以帧的形式发送）的确认信息后，才能认为发送成功。
  - 混合纠错是ARQ和FEC的结合，设计思想是对出现的错误尽量纠正，纠正不了则需要通过重发来消除差错。
  - 前向纠错接收端通过纠错解码自动纠正传输中出现的差错，所以该方法不需要重传。这种方法需要采用具有很强纠错能力的编码技术。

# 奇偶校验

■ 奇偶校验码是一种**最简单而有效**的数据校验方法。

■ **实现方法**: 在每个被传送码的左边或右边加上1位奇偶校验位0或1, 若采用奇校验位, 只需把每个编码中1的个数凑成奇数; 若采用偶校验位, 只要把每个编码中1的个数凑成偶数。

■ **检验原理**: 这种编码能发现1个或奇数个错, 但因码距较小, 不能实现错误定位。

■ **对奇偶校验码的评价**: 它能发现一位或奇数个位出错, 但无错误定位和纠错能力。尽管奇偶校验码的检错能力较低, 但对出错概率统计, 其中70~80%是1位错误, 另因奇偶校验码实现简单, 故它还是一种应用最广泛的校验方法。

■ **实际应用中**, 多采用**奇校验**, 因奇校验中不存在全“0”代码, 在某些场合下更便于判别。

0000**1**  
0001**0**  
0010**0**  
0011**1**  
0100**0**  
0101**1**  
0110**1**  
→ 0111**0**  
1000**0**  
1001**1**  
1010**1**  
1011**0**  
1100**1**  
1101**0**  
1110**0**  
1111**1**

## 奇偶监督码

奇偶监督码可分为奇数监督码和偶数监督码，两者的原理相同。

(1) 偶数监督码：监督位只有一位，使得码组中“1”的个数为偶数，即满足

$$a_{n-1} \oplus a_{n-2} \oplus \cdots \oplus a_0 = 0 \quad a_0 \text{ 为监督位}$$

**它能检测奇数个错码，无纠错能力。**

例 收端：1001 1011，则可能发生了奇数个错码

发端可能为      0001 1011、1101 1011  
                         0111 1011

错1位  
错3位

(2) 奇数监督码：监督位也只有一位，使得码组中“1”的个数为奇数，即满足  
它也能检测奇数个错码，无纠错能力。

$$a_{n-1} \oplus a_{n-2} \oplus \cdots \oplus a_0 = 1$$

**编码效率：(n-1)/n**

$$R=d/(d+r)$$

其中， $d$ 是信息元的个数， $r$ 为校验码个数

**应用：适用于一般随机错误的检测**



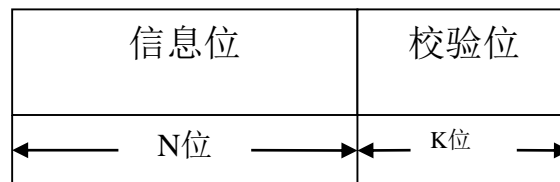
# 循环冗余校验码

## (Cyclic Redundancy Check ,CRC)

- CRC码是一种检错、纠错能力很强的数据校验码,主要用于网络、同步通信及磁表面存储器等应用场合。

### 1. 循环冗余校验码的编码方法

- 循环冗余校验码由两部分组成,左边为信息位,右边为校验位。若信息位为N位,校验位为K位,则该校验码被称为(N+K, N)码。



循环冗余校验码的格式

任意一个由二进制位串组成的代码都可以和一个系数仅为**0**和**1**取值的多项式一一对应，即把一个长度为**n**的代码可以表示为：

$$T(X) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1x + a_0$$

例：**1100101**

$$T(X) = 1 \cdot x^6 + 1 \cdot x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x^1 + 1$$

# CRC码（循环冗余码）——较强的检错能力，硬件实现简单

## □ 算法步骤

$M(X)$ 系数序列：11110111

$G(X)$ 系数序列：10011

附加 4 个零后形成的串：111101110000

$$\begin{array}{r}
 \begin{array}{l} X^r M(X)/G(X) \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ R(X) \end{array}
 \begin{array}{r}
 10011 \overline{) 111101110000} \\
 \text{XOR} \quad 10011 \\
 \hline
 11011 \\
 \text{XOR} \quad 10011 \\
 \hline
 10001 \\
 \text{XOR} \quad 10011 \\
 \hline
 10100 \\
 \text{XOR} \quad 10011 \\
 \hline
 11100 \\
 \text{XOR} \quad 10011 \\
 \hline
 1111 \longleftarrow \text{余数}
 \end{array}
 \end{array}$$

$T(X)$ 系数序列：111101111111



# 防碰撞

# 一、产生碰撞的原因

1

## 什么是碰撞

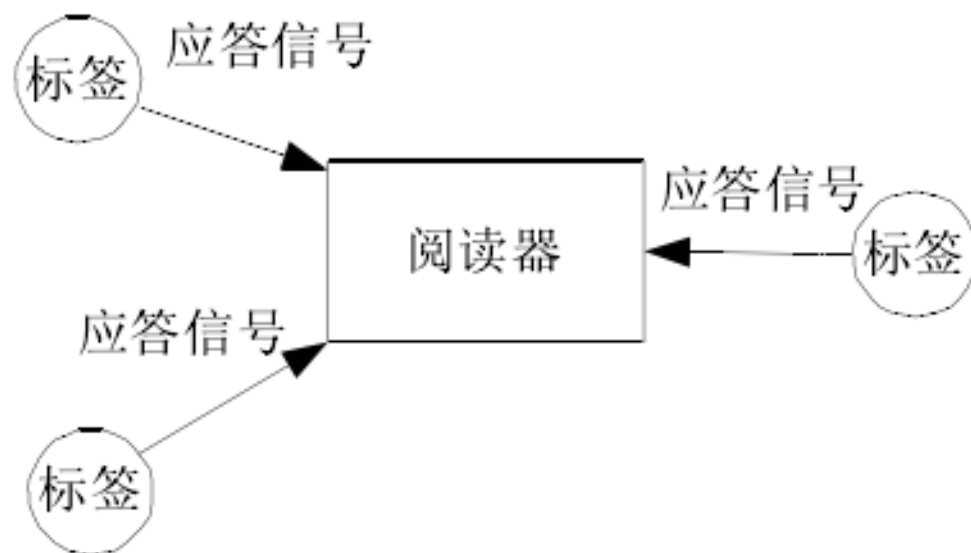
在RFID系统应用中，因为多个读写器或多个标签，造成的读写器之间或标签之间的相互干扰，统称为碰撞。

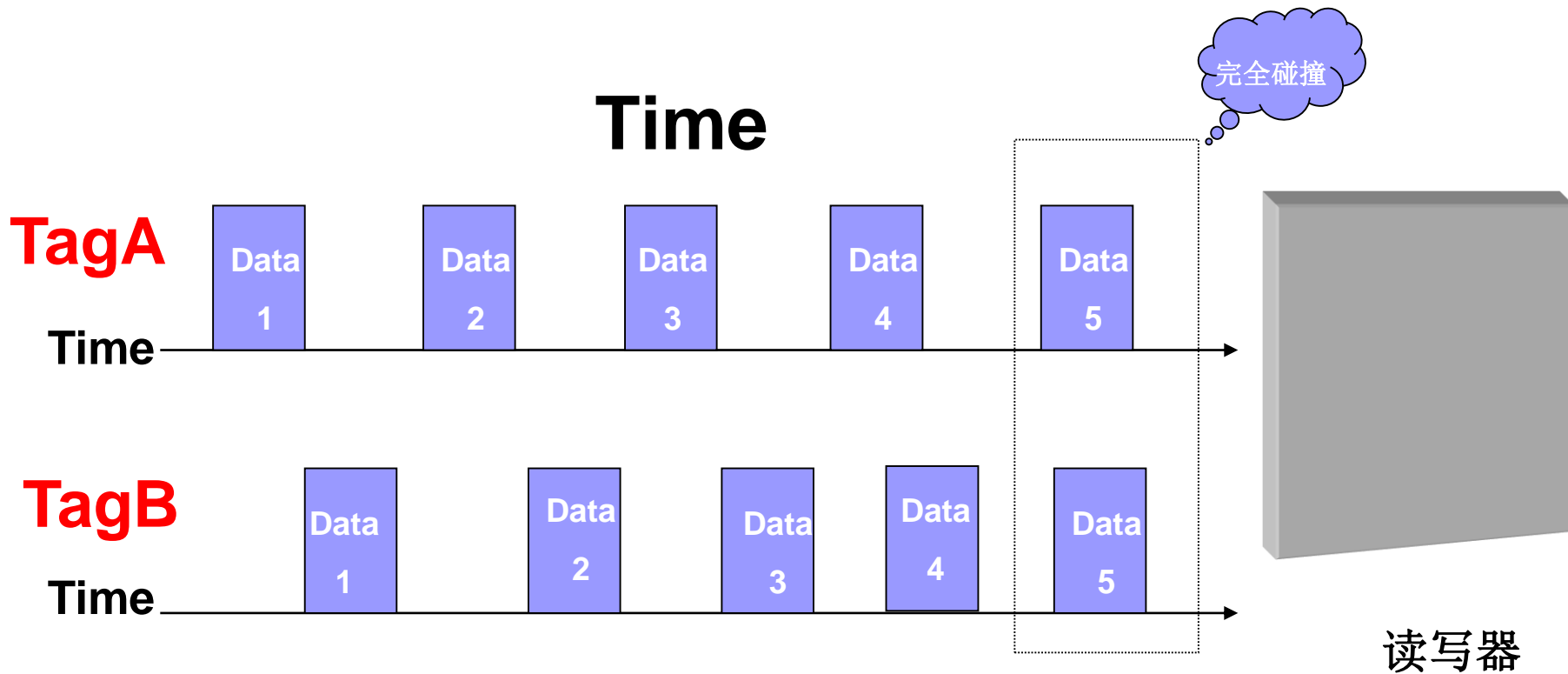
2

## 碰撞的类型

- 1、标签碰撞
- 2、读写器碰撞

# 标签碰撞

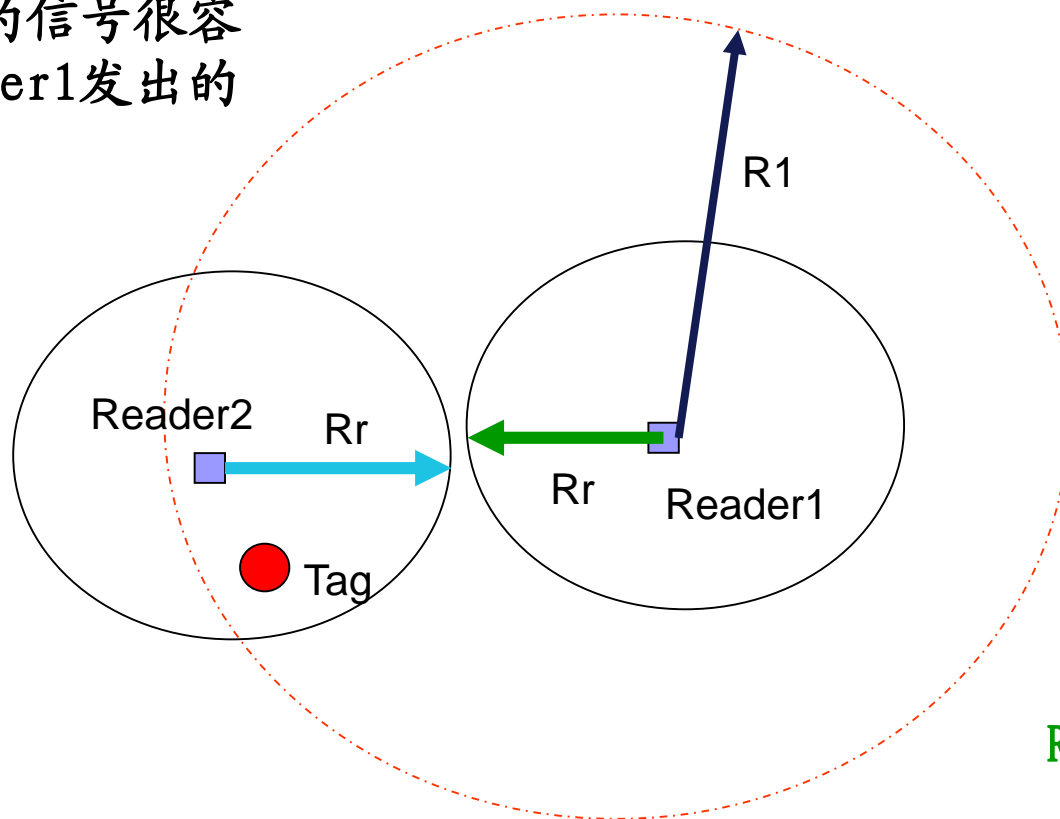




RFID数据碰撞示意图

# 读写器碰撞

从标签T反射到读写器Reader2的信号很容易被从Reader1发出的信号干扰。



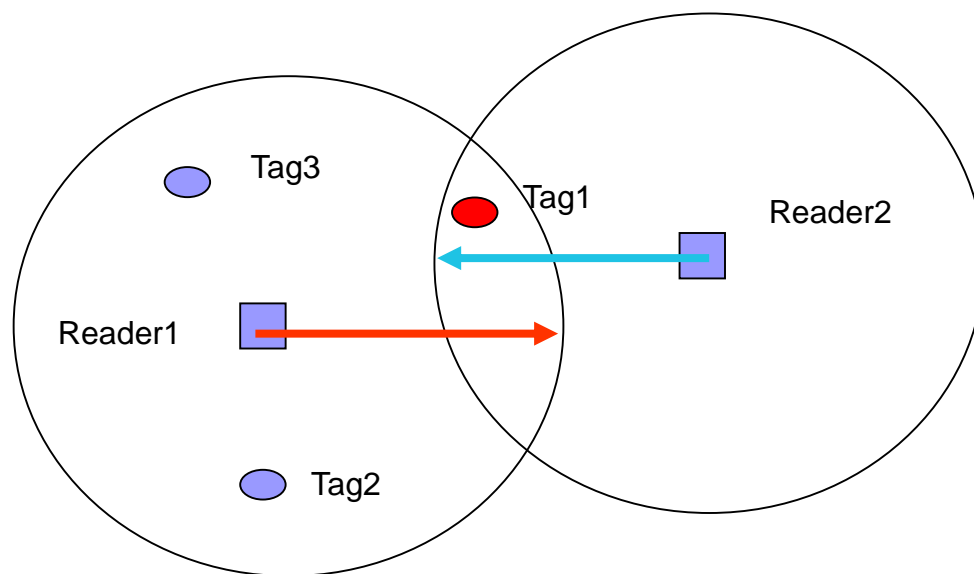
R1为Reader1的  
干扰范围

Rr为Reader1和  
Reader2的读取范围

读写器-读写器频率干扰



标签1接收到的信息为两个读写器发射信号的矢量和,是一个未知信号。



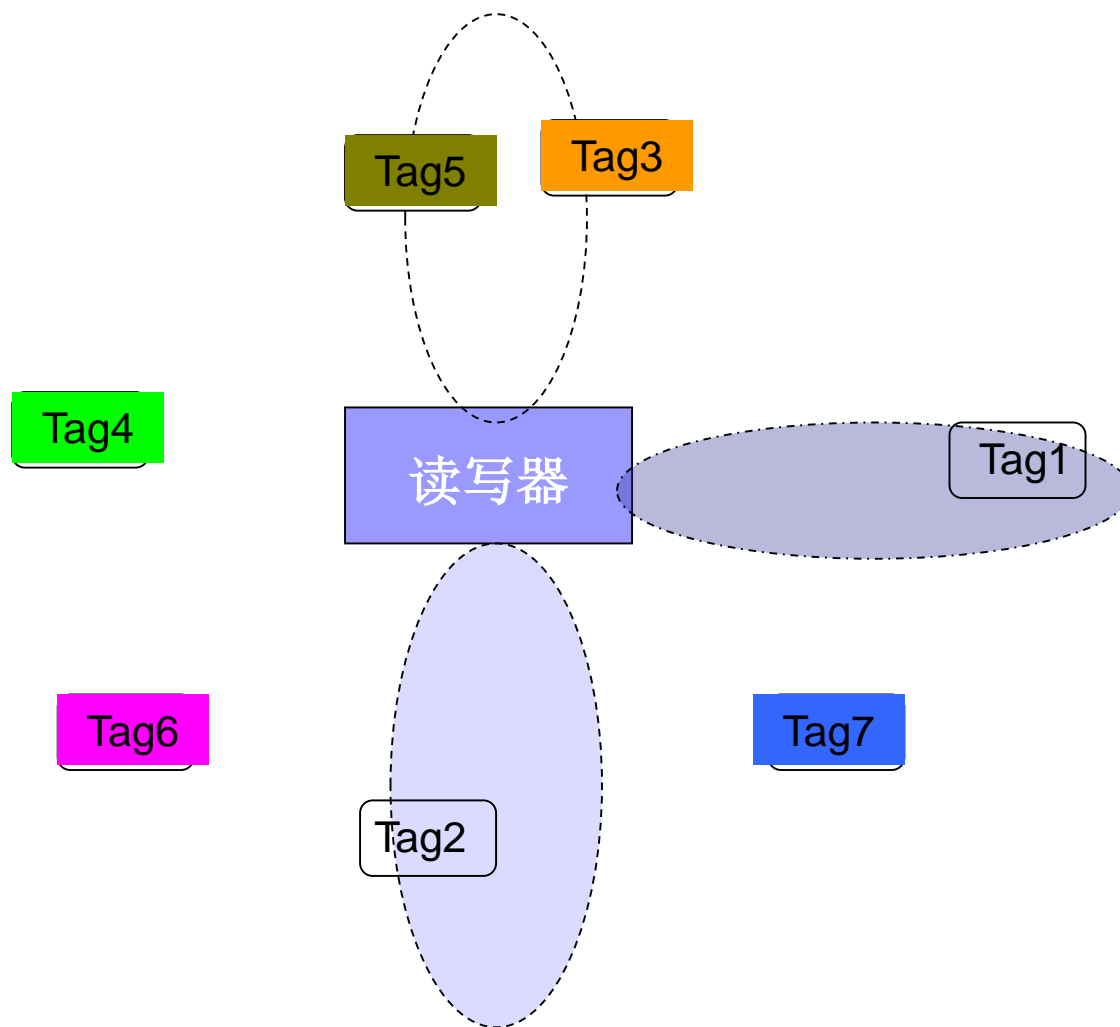
多读写器一标签干扰

## 二、防碰撞机制的实现

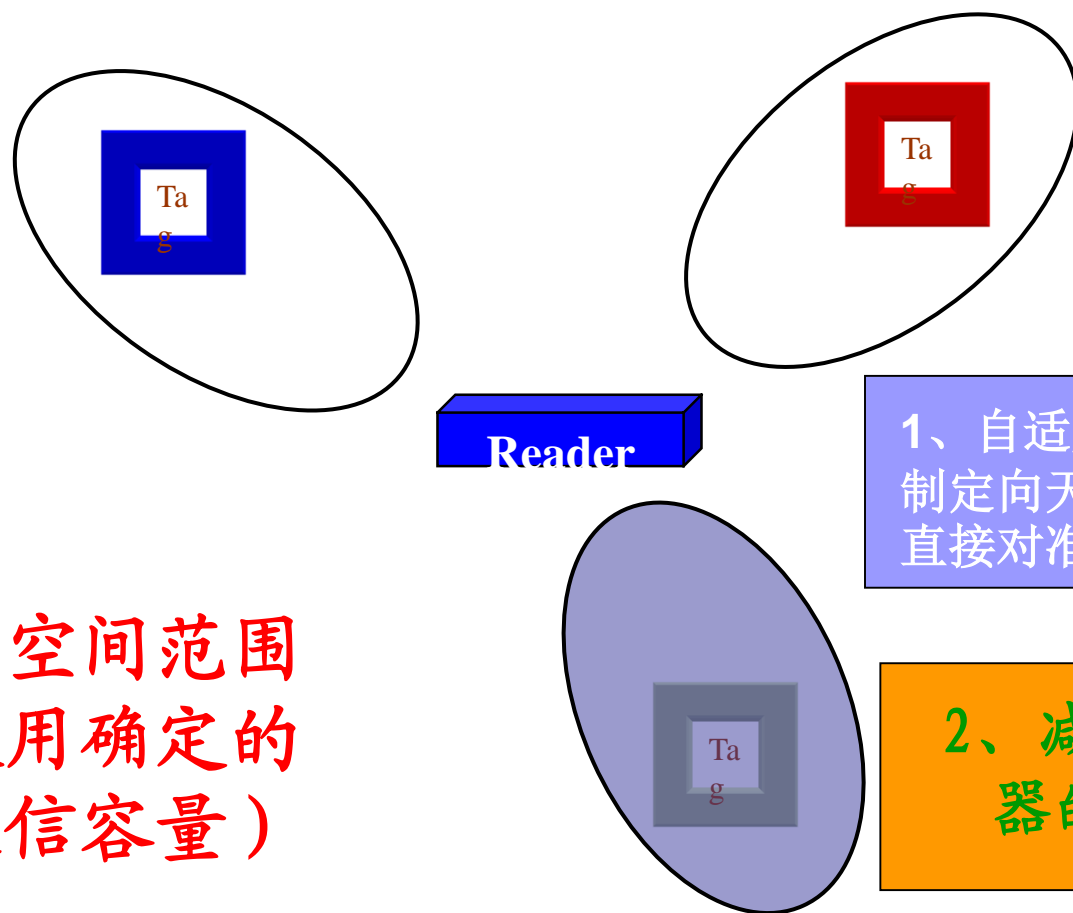
无线通信技术中，通信碰撞的四种解决防碰撞方法：

- ✓ 空分多址 (SDMA)
- ✓ 频分多址 (FDMA)
- ✓ 码分多址 (CDMA)
- ✓ 时分多址 (TDMA)

# 1、空分多址SDMA法



# 空间分割多重存取

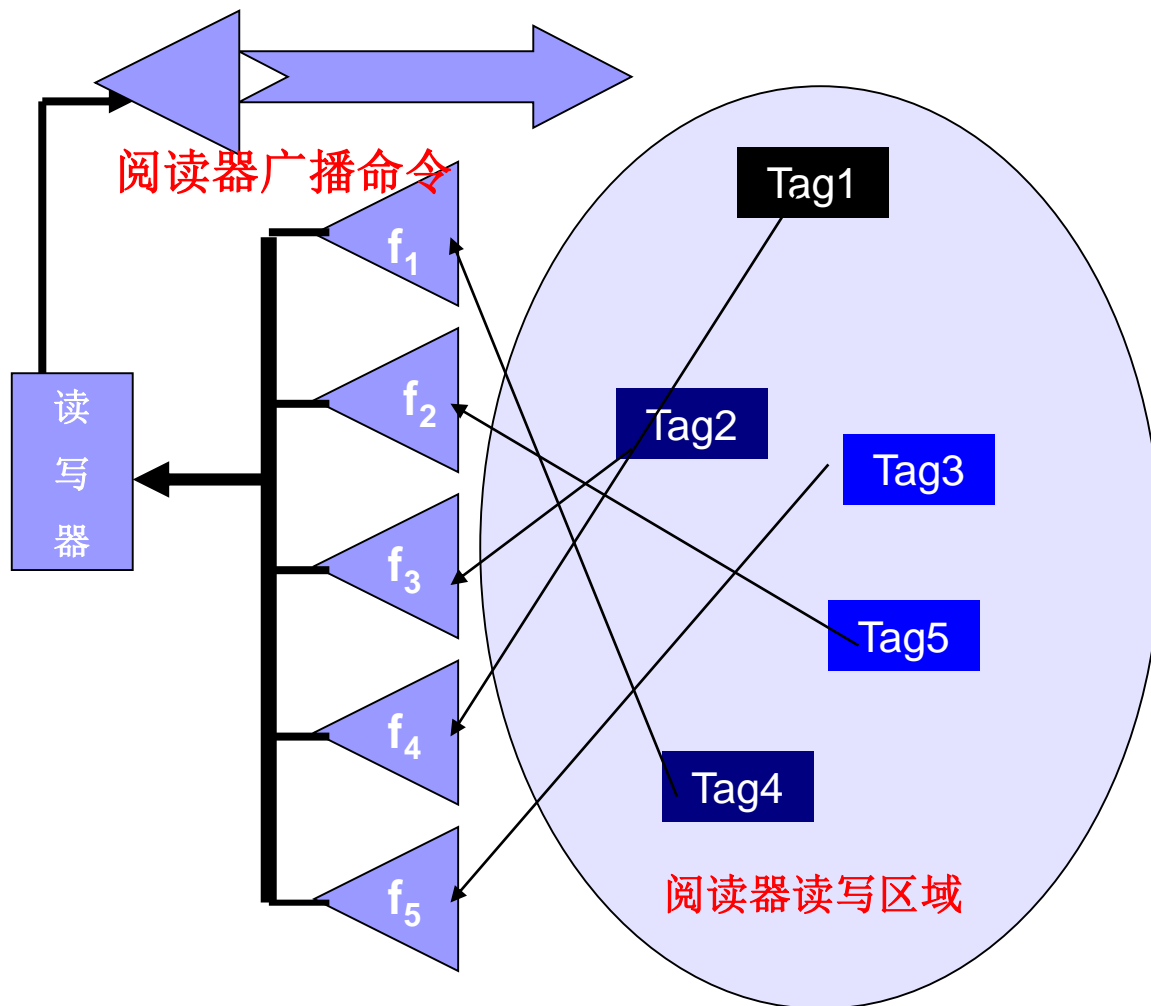


分离的空间范围  
内重新使用确定的  
资源（通信容量）

1、自适应SDMA，电子控制定向天线，天线的方向直接对准某个标签

2、减少单个读写器的作用范围

## 2、频分多址FDMA法

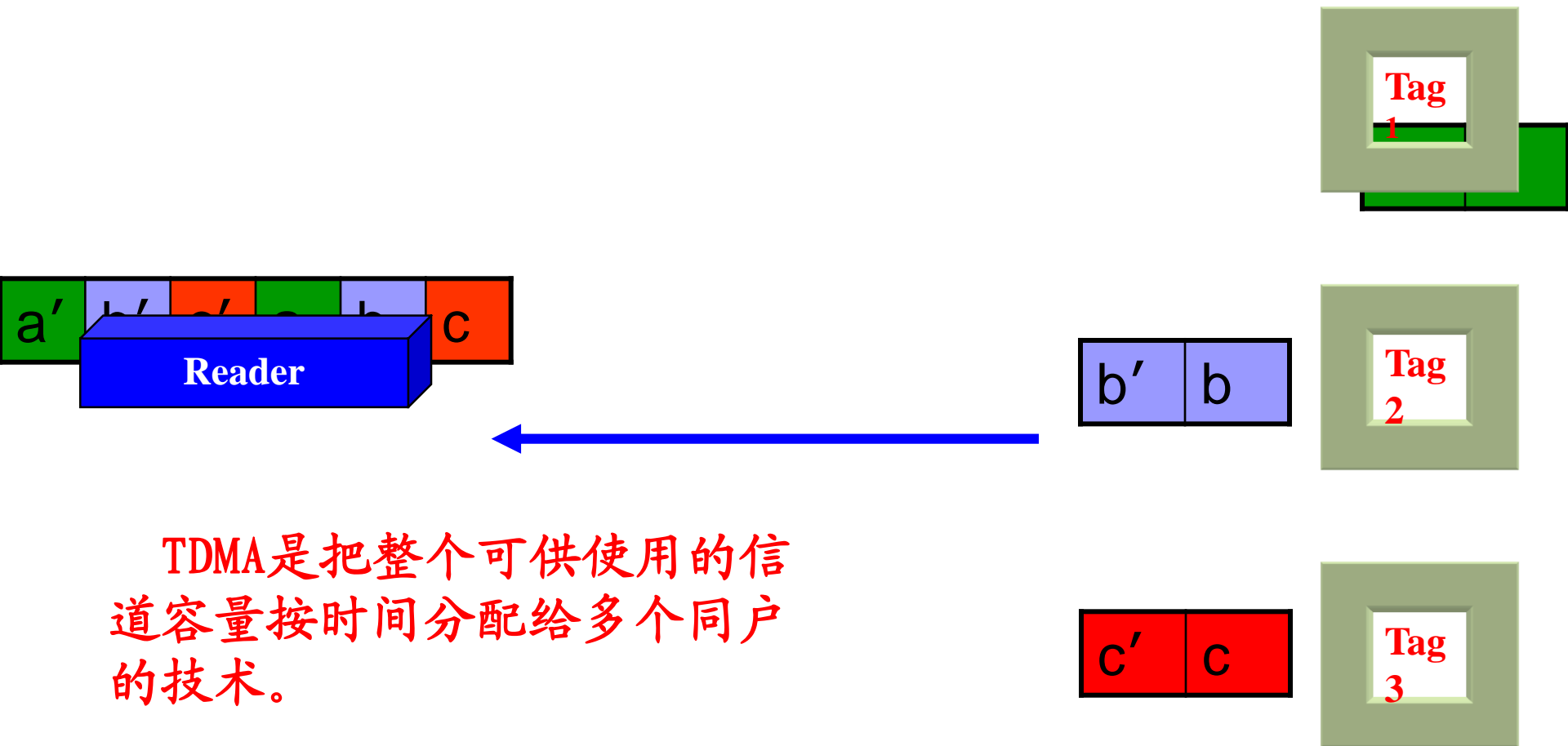


### 3、码分多址(CDMA)

不同用户传输信息所用的信号不是靠频率不同或时隙不同来区分，而是用各自不同的编码序列来区分，或者说，靠信号的不同波形来区分。如果从频域或时域来观察，多个CDMA信号是互相重叠的。CDMA是利用不同的码序列分割成不同信道的多址技术。

CDMA的频带利用率低，信道容量较小，地址码选择较难、接收时地址码捕获时间较长，其通信频带和技术复杂性在RFID系统中难以应用。

## 4、时间分割TDMA



## ■ 防碰撞算法

- **非确定性算法**也称**标签控制法**，在该方法中，读写器没有对数据传输进行控制，标签的工作是非同步的，**标签获得处理的时间不确定**，因此标签存在“**饥饿**”问题。

**ALOHA**算法是一种典型的非确定性算法，实现简单，广泛用于解决标签的碰撞问题。

- **确定性算法**也称**读写器控制法**，由**读写器观察控制**所有标签。按照规定算法，在读写器作用范围内，首先选中一个标签，在同一时间内读写器与一个标签建立通信关系。**二进制树型搜索算法**是典型确定性算法，该类算法比较复杂，识别时间较长，但无标签饥饿问题。



### 三、防碰撞算法

#### 1、ALOHA防碰撞算法

- 各种ALOHA算法：纯ALOHA算法、时隙ALOHA算法、帧时隙ALOHA算法、动态帧时隙ALOHA算法。

# ALOHA算法

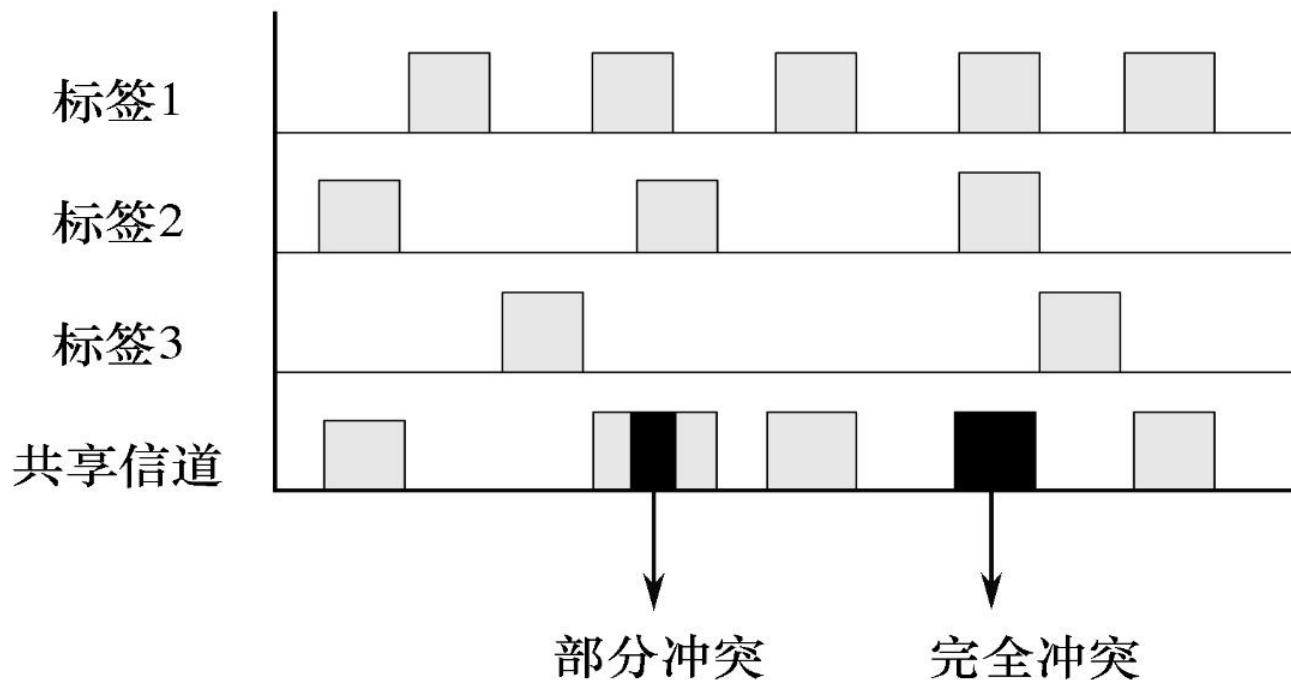
## 纯ALOHA算法

- ❑ 读写器检测出信号存在干扰，向电子标签发出命令停止传输信号；
- ❑ 电子标签经历一个随机时间段内的待命状态后，重新向读写器发送信息
- ❑ 各个电子标签待命时间片段长度是随机的，再次向读写器发送信号的时间也不相同，减少碰撞
- ❑ 读写器成功识别某个标签后，会令该标签进入休眠状态。而其他标签则会一直对读写器所发出命令进行响应，并重复发送信息给读写器，当标签被识别后，就会一一进入到休眠状态，直到读写器识别出所有在其工作区内的标签。

## ■ 纯ALOHA算法

纯ALOHA算法中的信号碰撞分两种情况：

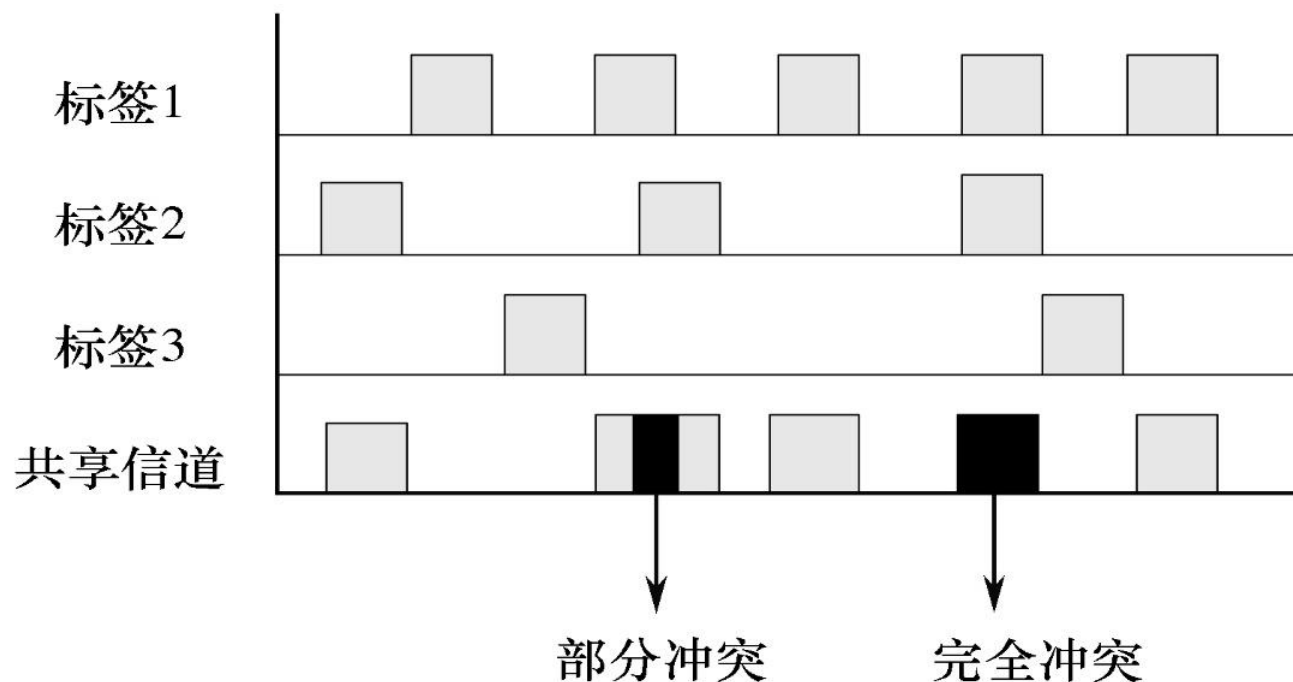
- (1) 一种是信号部分碰撞，即信号的一部分发生了冲突；
- (2) 一种则是信号的完全碰撞，是指数据完全发生了冲突。



假设一帧信息的长度为  $T_0$  ,起始时间为  $t_0$  , 另一帧的起始时间  $t_1$

**会发生碰撞时间  $t_0 - T_0 \leq t_1 \leq t_0 + T_0$**

**碰撞时间长度  $2T_0$**



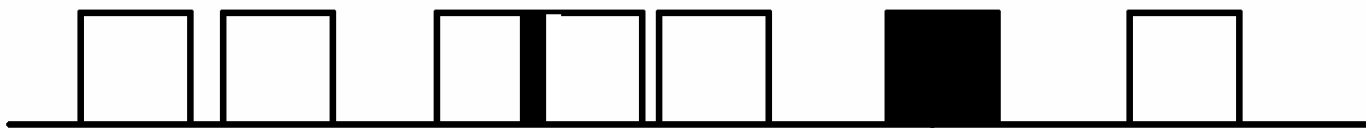
标签1



标签2



信道



部分冲突

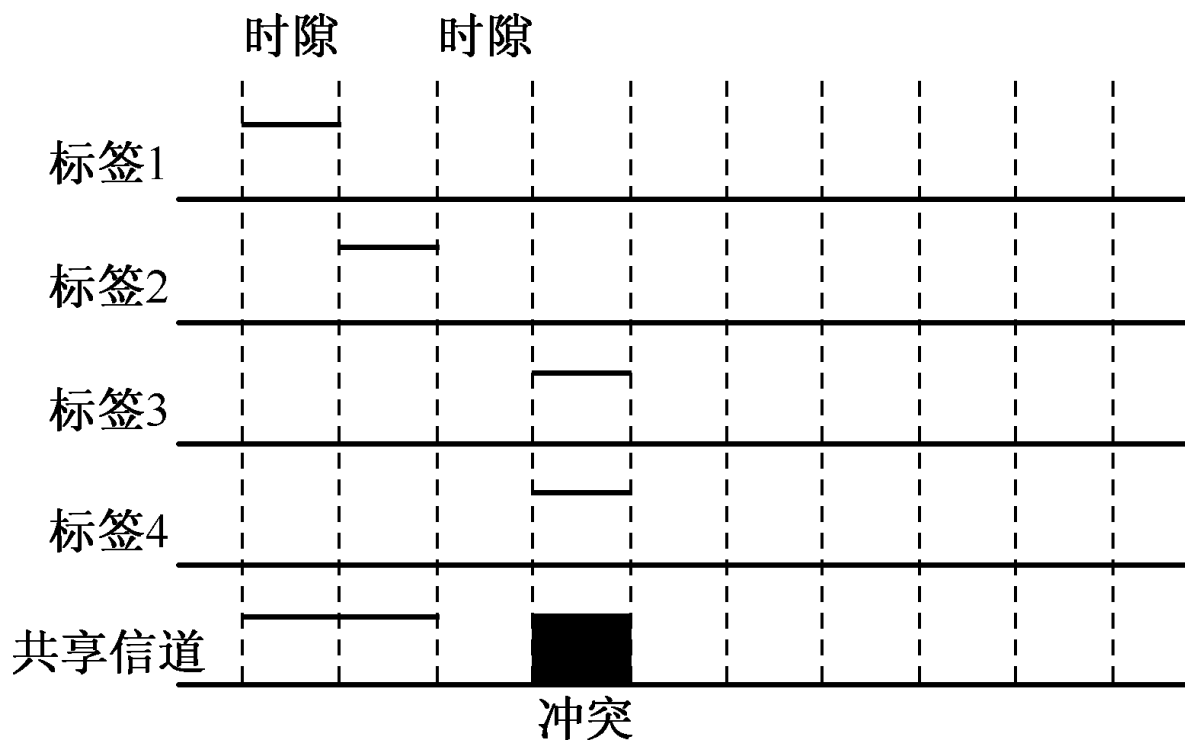
完全冲突

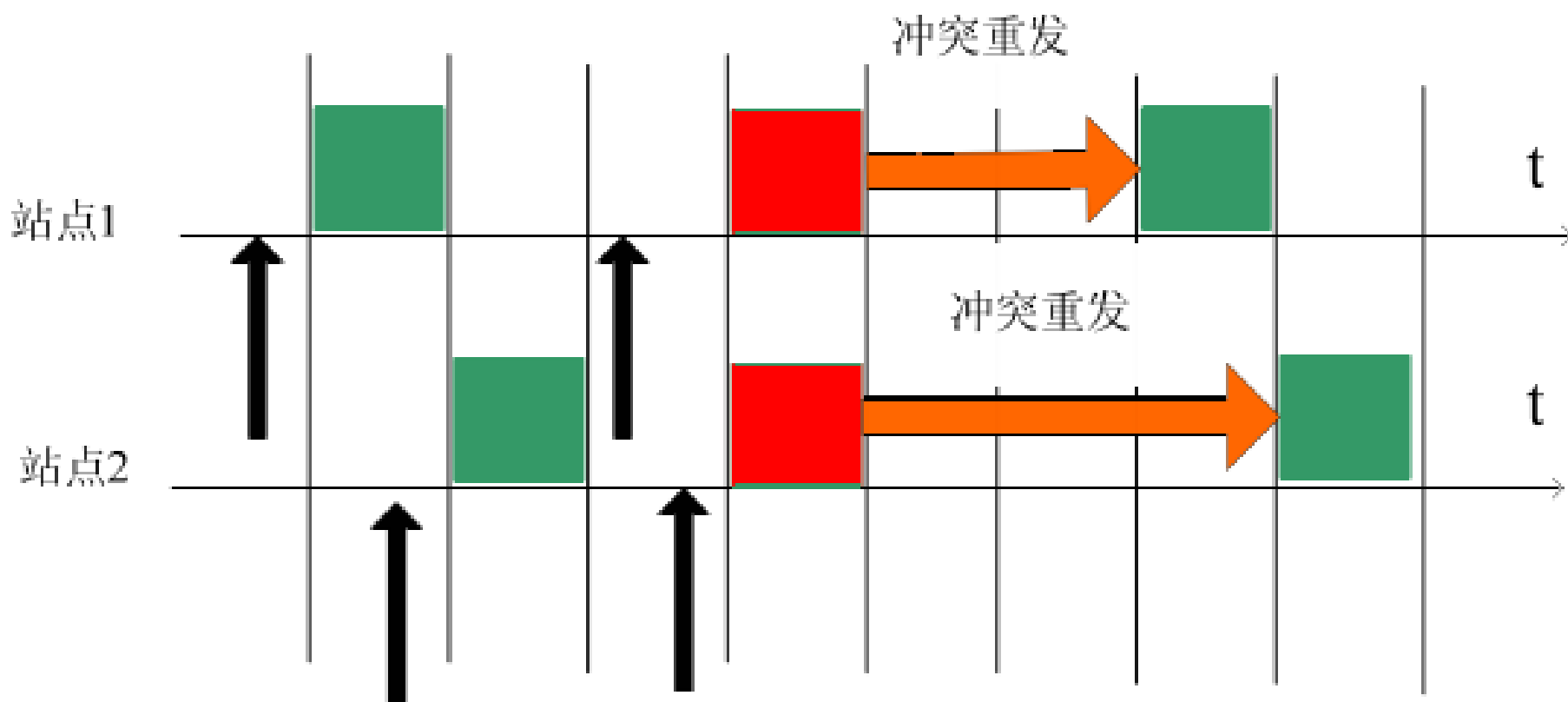
ALOHA算法的模型图

## 时隙ALOHA算法

在ALOHA算法的基础上把时间分成多个离散时隙(slot)，并且每个时隙长度要大于标签回复的数据长度，标签只能在每个时隙内发送数据。每个时隙存在：

- a 空闲时隙：此时隙内没有标签发送
- b 成功识别时隙：仅一个标签发送且被正确识别
- c 碰撞时隙：多个标签发送，产生碰撞





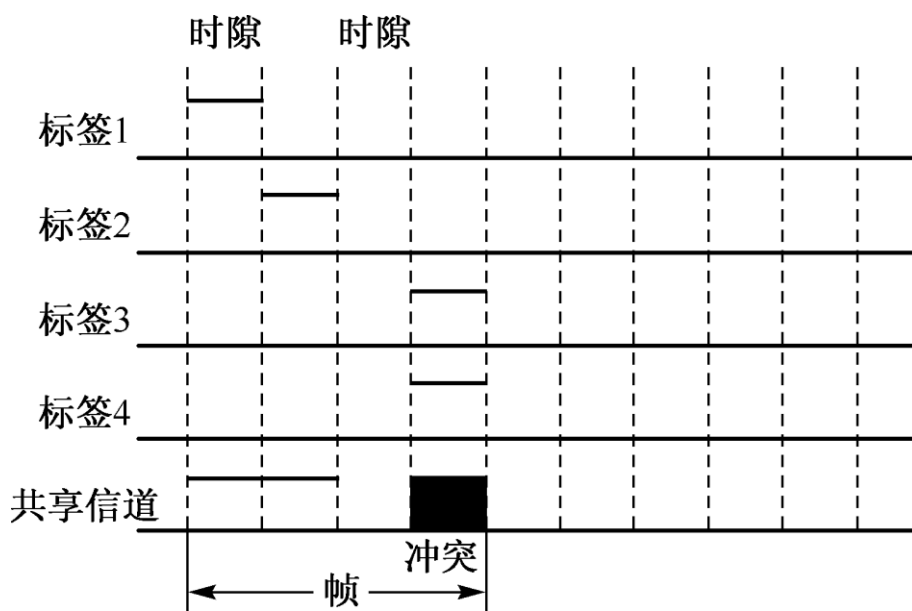
时隙ALOHA算法示意图

## 帧时隙ALOHA算法

在时隙ALOHA算法基础上把N各时隙组成一帧，**标签在每个帧内随机选择一个时隙发送数据**。当阅读器发送读取命令后，等待标签回答。每个时隙的长度足够一个标签回答完，当在一个时隙中只有一个标签回答时，阅读器可以分辨出标签；当没有回答时跳过该时隙；当多个标签回答时，发生碰撞，需重新读取。

该算法特点：

- a 把N个时隙打包成一帧；
- b 标签在每N个时隙中只随机发送一次信息；
- c 需要阅读器和标签之间的同步操作，每个时隙需要阅读器进行同步。





## ■ 动态帧时隙ALOHA算法

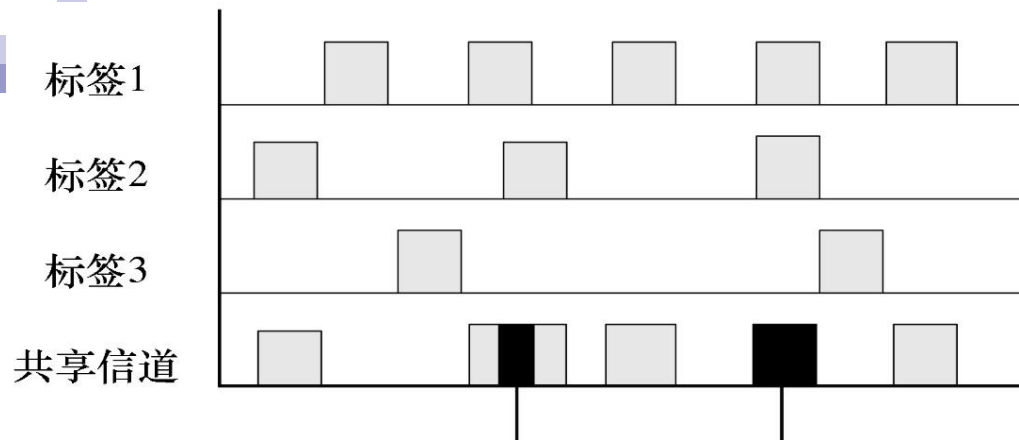
思路：一个帧内的时隙数目 $N$ 能随阅读区域中的标签的数目而动态改变，或通过增加时隙数以减少帧中的碰撞数目。

步骤：（1）进入识别状态，在开始识别命令中包含了初始的时隙数 $N$ 。

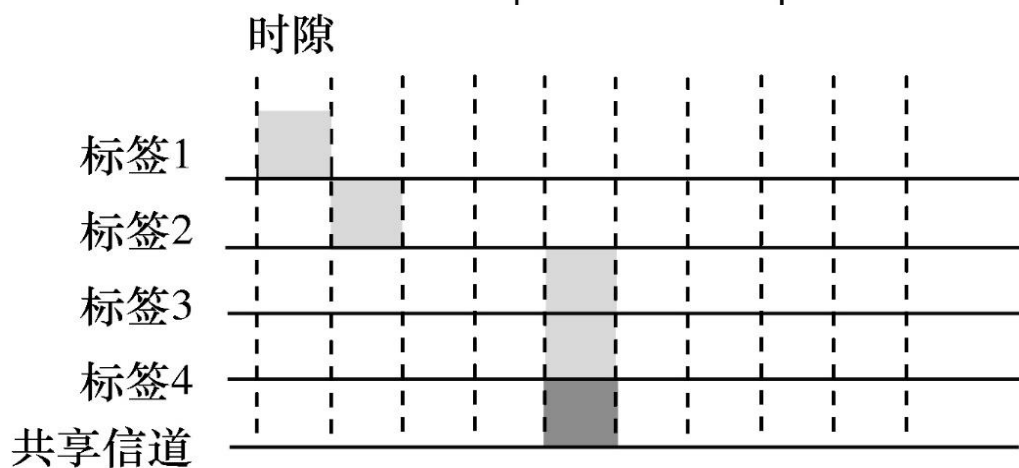
（2）由内部伪随机数发生器为进入识别状态的标签随机选择一个时隙，同时将自己的时隙计数器复位为1。

（3）当标签随机选择的时隙数等于时隙计数器时，标签向阅读器发送数据，当不等时，标签将保留自己的时隙数并等待下一个命令。

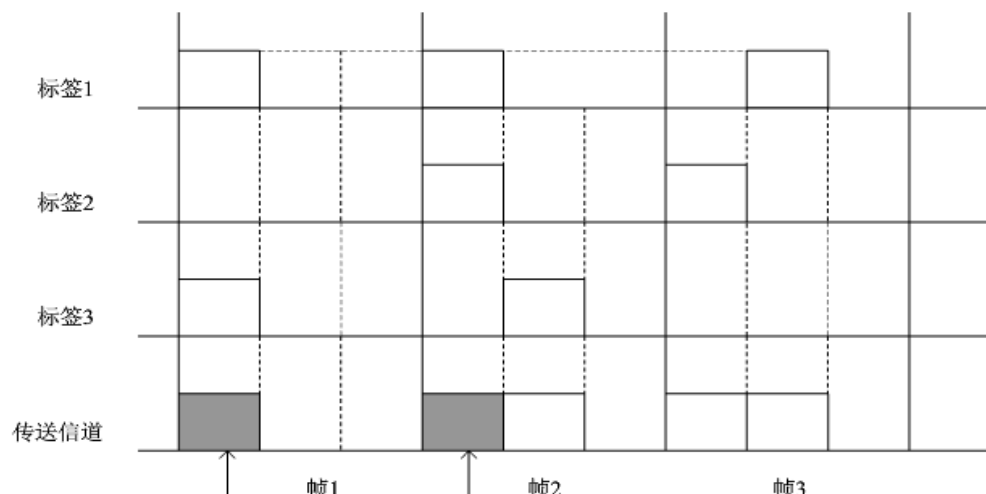
（4）当阅读器检测到的时隙数量等于命令中规定的循环长度 $N$ 时，本次循环结束。阅读器转入（2）开始新的循环。



## 纯ALOHA算法



## 时隙ALOHA算法



## (动态) 帧时隙 ALOHA算法

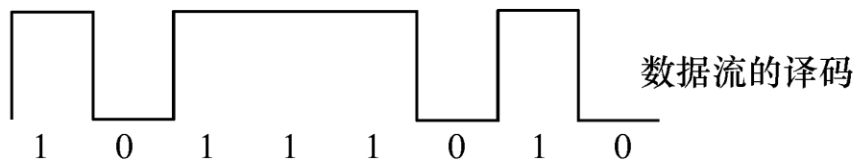
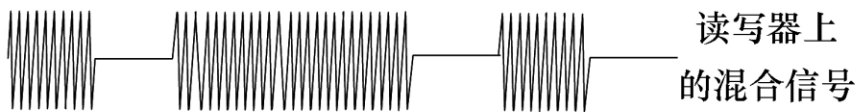
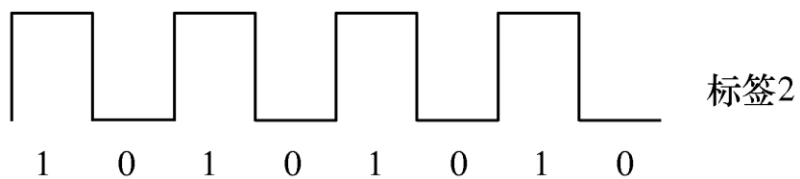
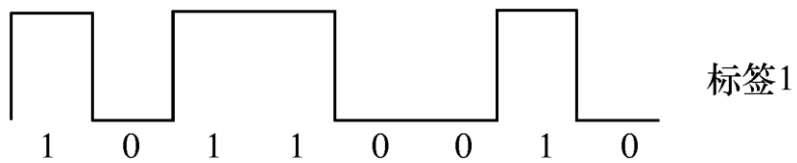
# 二进制树型搜索算法

二进制树型搜索算法由读写器控制，基本思想是不断的将导致碰撞的电子标签进行划分，缩小下一步搜索的标签数量，直到只有一个电子标签进行回应。

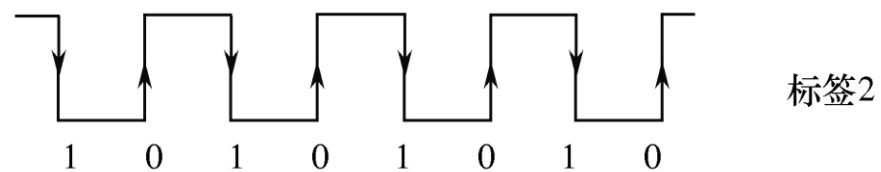
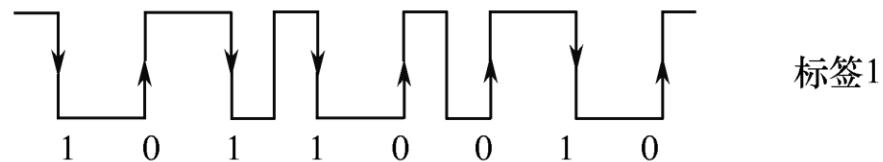
基本思路：多个标签进入读写器工作范围后，读写器发送带限制条件的询问命令，满足限制条件的标签回答，如果发生碰撞，则根据发生错误的位修改限制条件，再一次发送询问命令，直到找到一个正确的回答，并完成对该标签的读写操作。对剩余的标签重复以上操作，直到完成对所有标签的读写操作。

## 冲突位检测

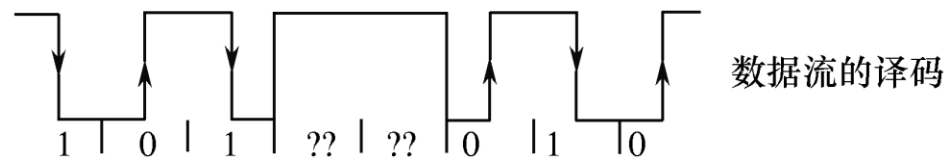
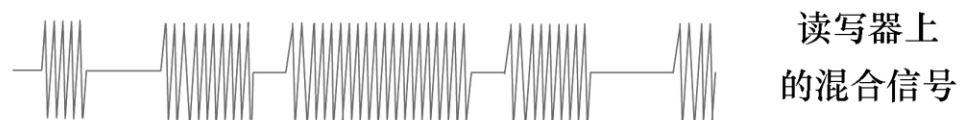
实现该算法系统的必要前提是能够辨认出在读写器中数据冲突位的



(a)NRZ编码



<http://blog.csdn.net/yixuoming>

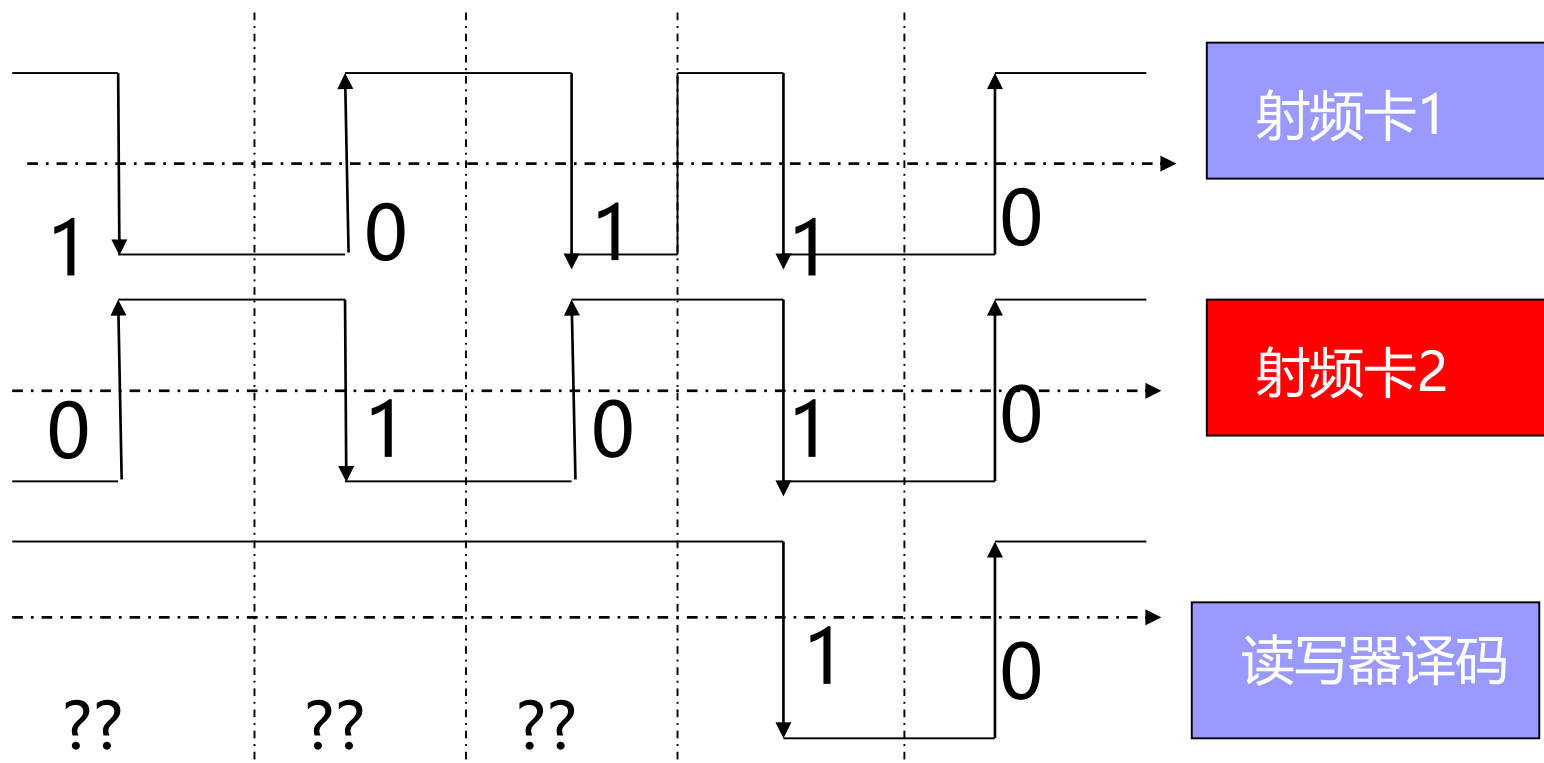


(b)曼彻斯特编码

曼彻斯特码可检测碰撞位

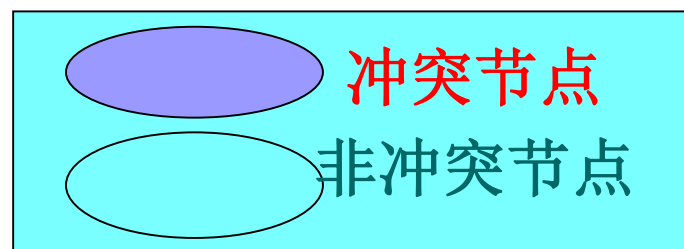
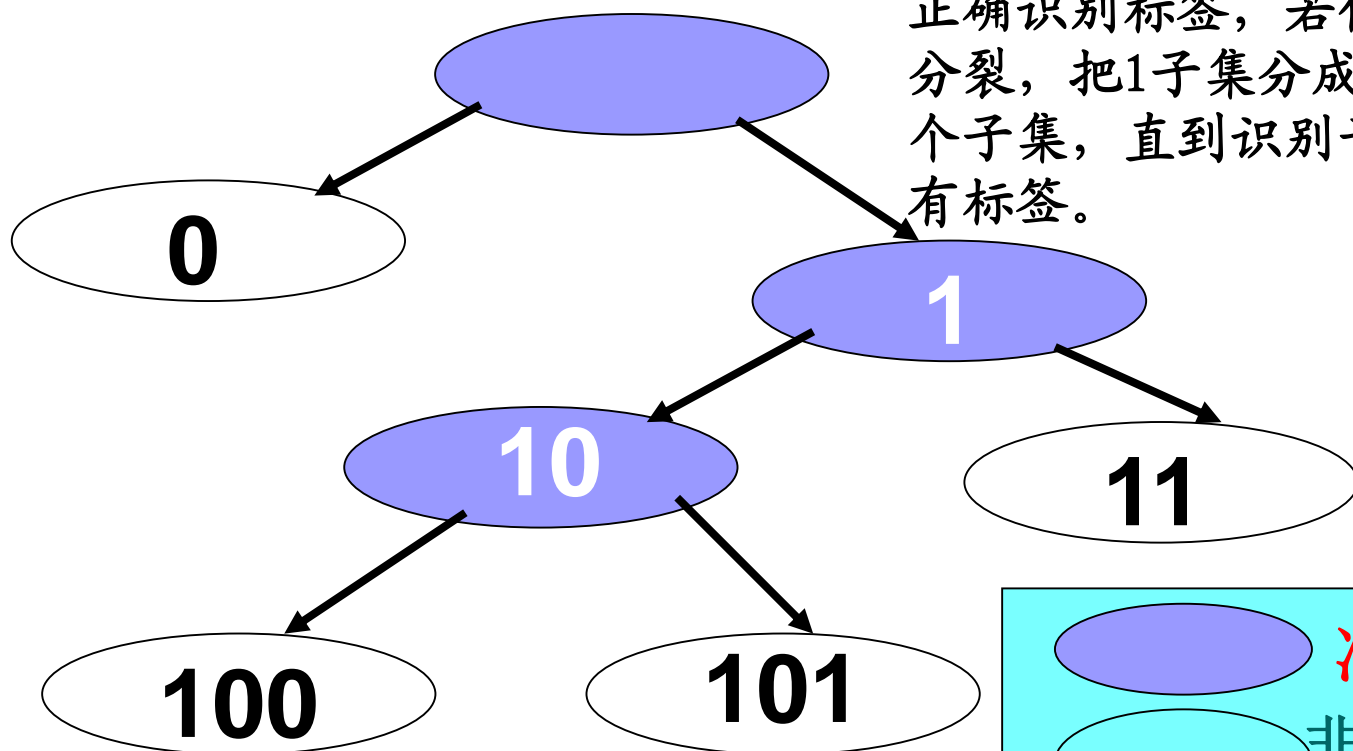
## 如何确定碰撞的准确比特位置？

**曼彻斯特码**(Manchester)可在多卡同时响应时，译出错误码字，可以按位识别出碰撞。这样可以  
根据碰撞的位置，按一定法则重新搜索射频卡。



## 2、二进制树型搜索算法

**基本思想是：**将处于碰撞的标签分成左右两个子集0和1，先查询子集0，若没有碰撞，则正确识别标签，若仍有碰撞则分裂，把1子集分成00和01两个子集，直到识别子集1中所有标签。



向下传输 读写器→标签	请求 <=11111111	第一次迭代	请求 <10111111	第二次迭代	请求 <10101111	第三次迭代
向上传输		1x1x001x		101x001x		10100011
标签1	→	10110010	→	10110010		
标签2	→	10100011	→	10100011	→	10100011
标签3	→	10110011	→	10110011		
标签4	→	11100011				

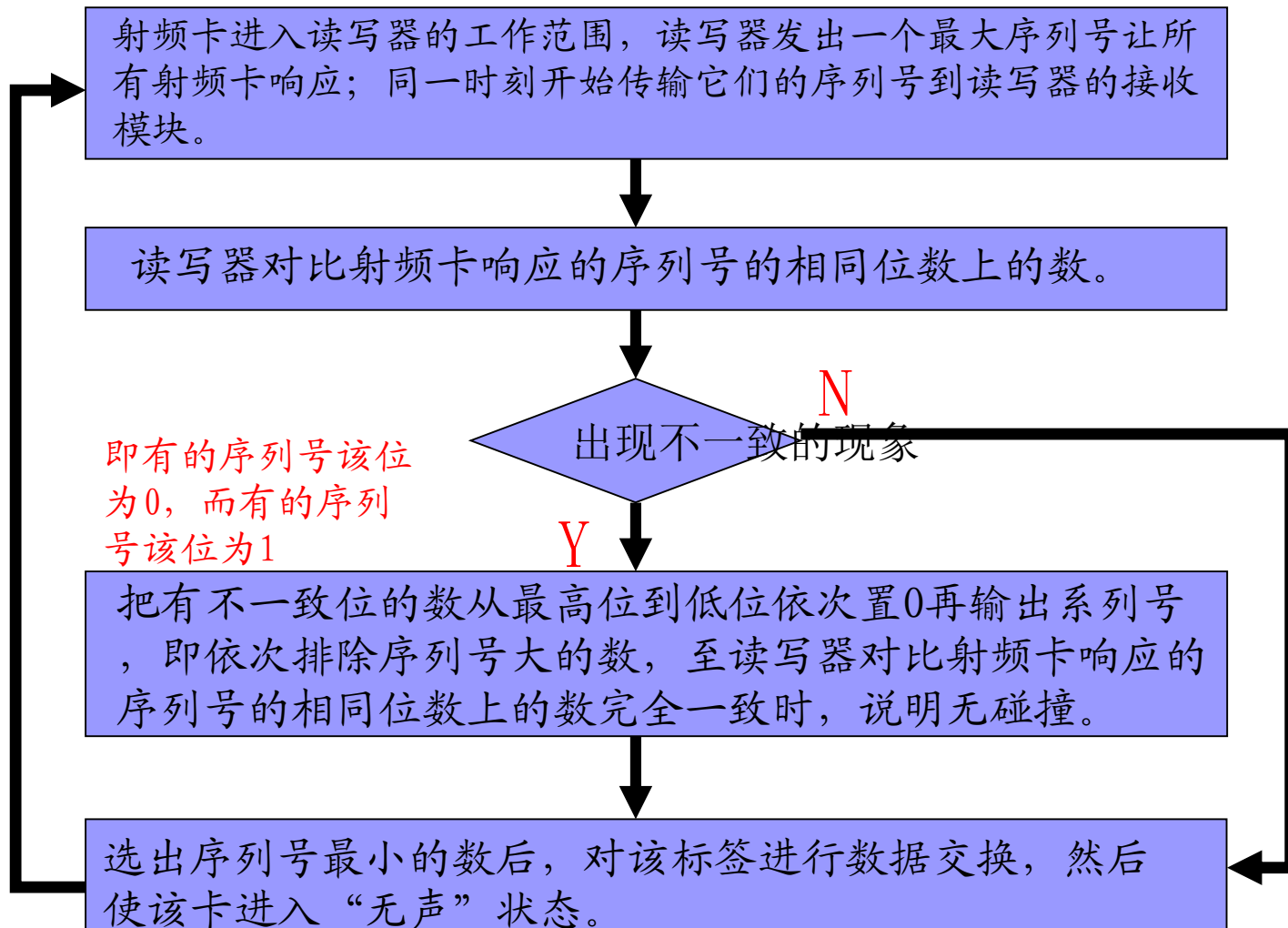
- 例：以如下三个在读写器作用范围内的电子标签为例说明二进制树型搜索算法选择电子标签的迭代过程。

假设这三个电子标签的序列号分别为：

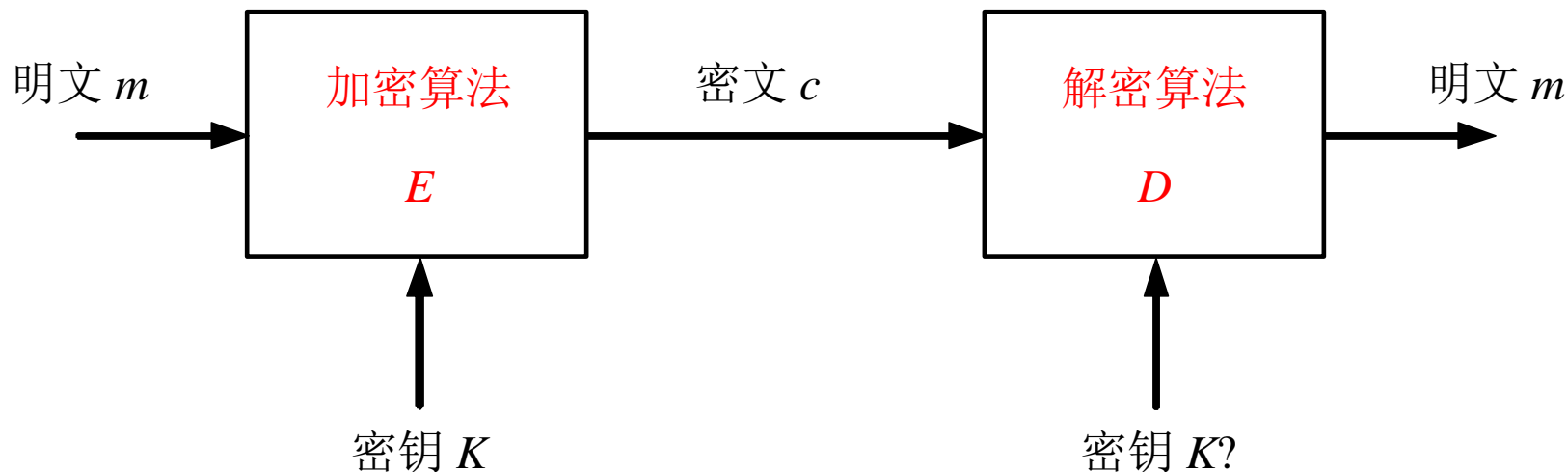
- 电子标签1：11100011
- 电子标签2：10100011
- 电子标签3：10110010



# 二进制搜索算法的工作流程是：



# 1. 密码学的基础概念



## 加密模型

加密和解密变换的关系式:

$$c = E_K(m) \quad m = D_K'(c) = D_K'(E_K(m))$$

# 对称密码体制

- 一种常规密钥密码体制，也称为单钥密码体制或私钥密码体制。在对称密码体制中，**加密密钥和解密密钥相同**。
- 从得到的密文序列的结构来划分，有序列密码和分组密码两种不同的密码体制。
  - **序列密码**是将明文 $m$ 看成是连续的比特流（或字符流） $m_1m_2\dots$ ，并且用密钥序列 $K=K_1K_2\dots$ 中的第 $i$ 个元素 $K_i$ 对明文中的 $m_i$ 进行加密，因此也称为流密码。
  - **分组密码**是将明文划分为固定的 $n$ 比特的数据组，然后以组为单位，在密钥的控制下进行一系列的线性或非线性的变化而得到密文。

**序列密码由于硬件实现容易，在RFID系统中获得了广泛应用。**

# 非对称密码体制

## □ 公开密钥与私人密钥

- 加密算法 $E$ 和解密算法 $D$ 必须满足以下三个条件：
- ①  $D(E(m)) = m$ ,  $m$ 为明文；
- ② 从 $E$ 导出 $D$ 非常困难；
- ③ 使用“选择明文”攻击不能破译，即破译者即使能加密任意数量的选择明文，也无法破译密文。

### 3、分组密码

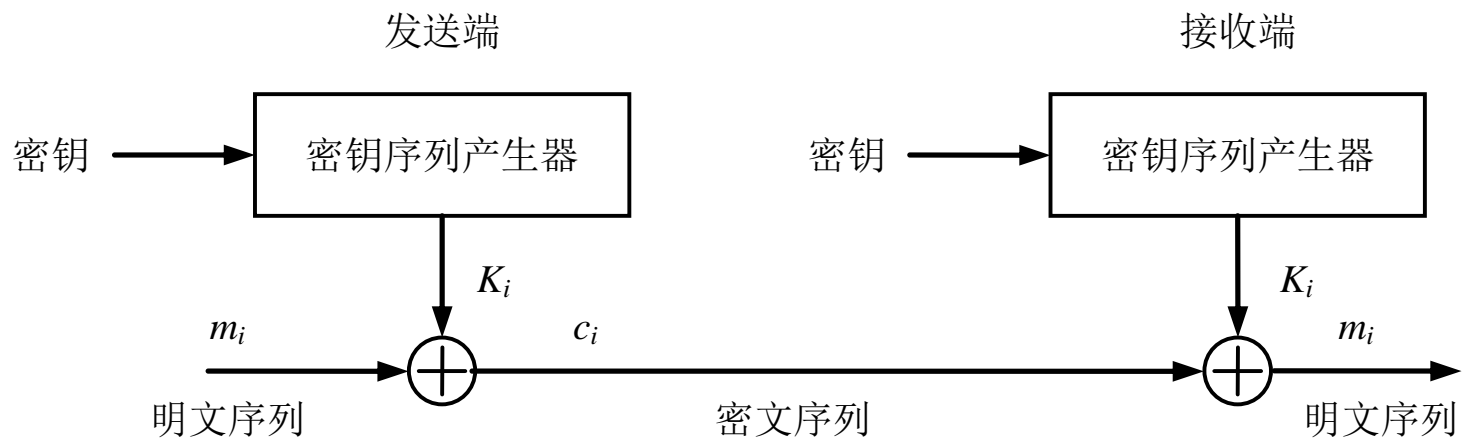
#### □ 数据加密标准（Data Encryption Standard, DES）

- DES由IBM公司1975年研究成功并发表，1977年被美国定为联邦信息标准。
- DES的分组长度为64位，密钥长度为56位，将64位的明文经加密算法变换为64位的密文。

#### □ 高级加密标准（Advanced Encryption Standard, AES）

- 新的加密标准，它是分组加密算法，分组长度为128位，密钥长度有128位、192位、256位三种，分别称为AES-128，AES-192，AES-256。

## ■ 序列密码体制



□ 密钥序列产生器进行初始化  $c_i = E(m_i) = m_i \oplus K_i$

□ 接收端，对  $c_i$  的解密算法

$$D(c_i) = c_i \oplus K_i = (m_i \oplus K_i) \oplus K_i = m_i$$

95 □ 需要同步