二、无线射频识别技术

欧阳元新

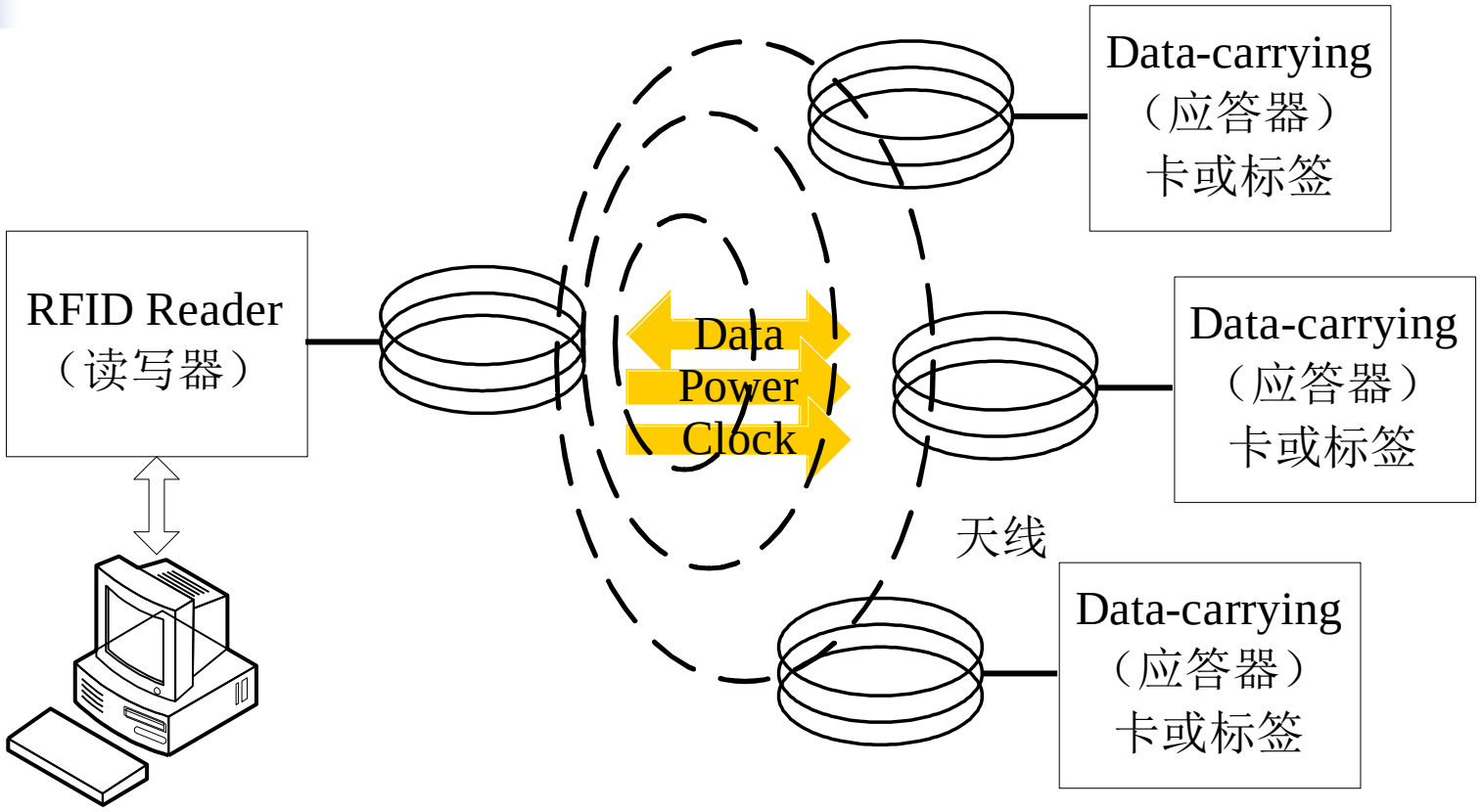
2020年9月21日

oyyx@buaa.edu.cn

无线射频识别技术
基本工作原理

无线射频识别技术（Radio Frequency Identification）是一种非接触的自动识别技术，其基本原理是利用射频信号和空间耦合（电感或电磁耦合）传输特性，实现对被识别物体的自动识别。

无线射频识别系统的基本构成



RFID技术发展历史

- 1941~1950：雷达的改进和应用催生RFID技术
- 1951~1960：早期技术探索阶段
- 1961~1970：理论得到发展，开始应用尝试
- 1971~1980：大发展时期，出现了最早的应用
- 1981~1990：进入商业应用阶段
- 1991~2000：广泛应用
- 2001年至今：RFID产品更加丰富，标准化问题为人们所重视。

RFID的优势

- 条码很容易污、损
- 标签可以防水
- 耐高温、可以抵御恶劣环境
- 防冲突
- 不必可见
- 可嵌入

RFID的分类

- 按标签的供电方式：
  - 有源系统：有源射频标签使用标签内的电池的能量，识别距离较长，可达几十米甚至上百米。寿命有限、价格高、体积较大、无法制作成薄卡。
  - 无源系统：无源射频标签不含有电池，利用耦合的读写器发射的电磁场能量作为自己的能量，重量轻、寿命长、体积小、很便宜、识别距离较短，一般是几厘米到几米。

RFID的分类

- 按标签的数据调制方式：
  - 主动式：有源系统为主动式
  - 被动式：无源系统是被动式
  - 半主动式：半主动标签本身内部也带有电池，只起到对标签内部数字电路供电，但是标签不通过自身的能量主动发射数据

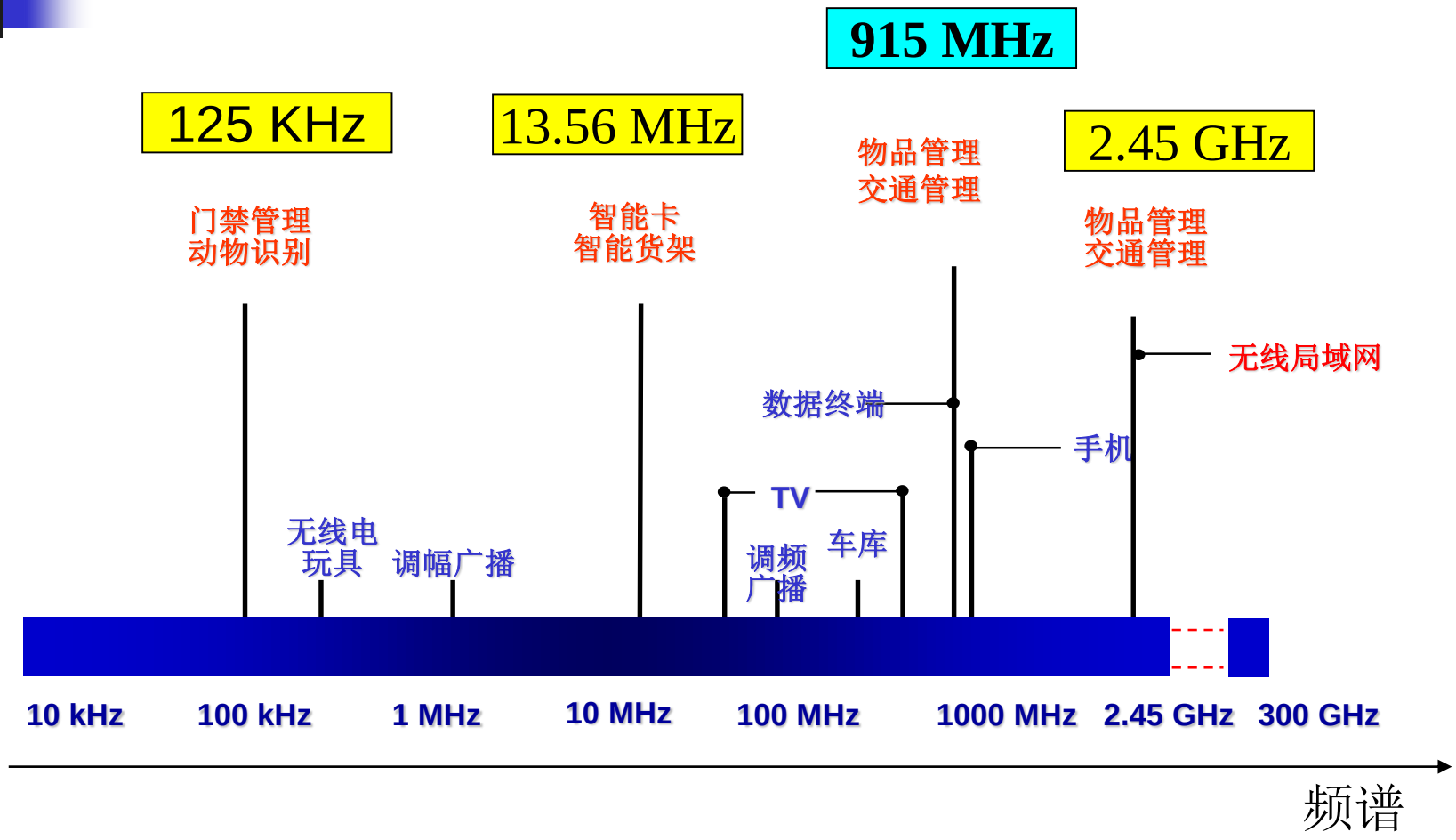
RFID的分类

- 按标签可读写性：
  - 可读写标签
  - 一次写入多次读取标签
  - 只读标签

RFID的分类--工作频率

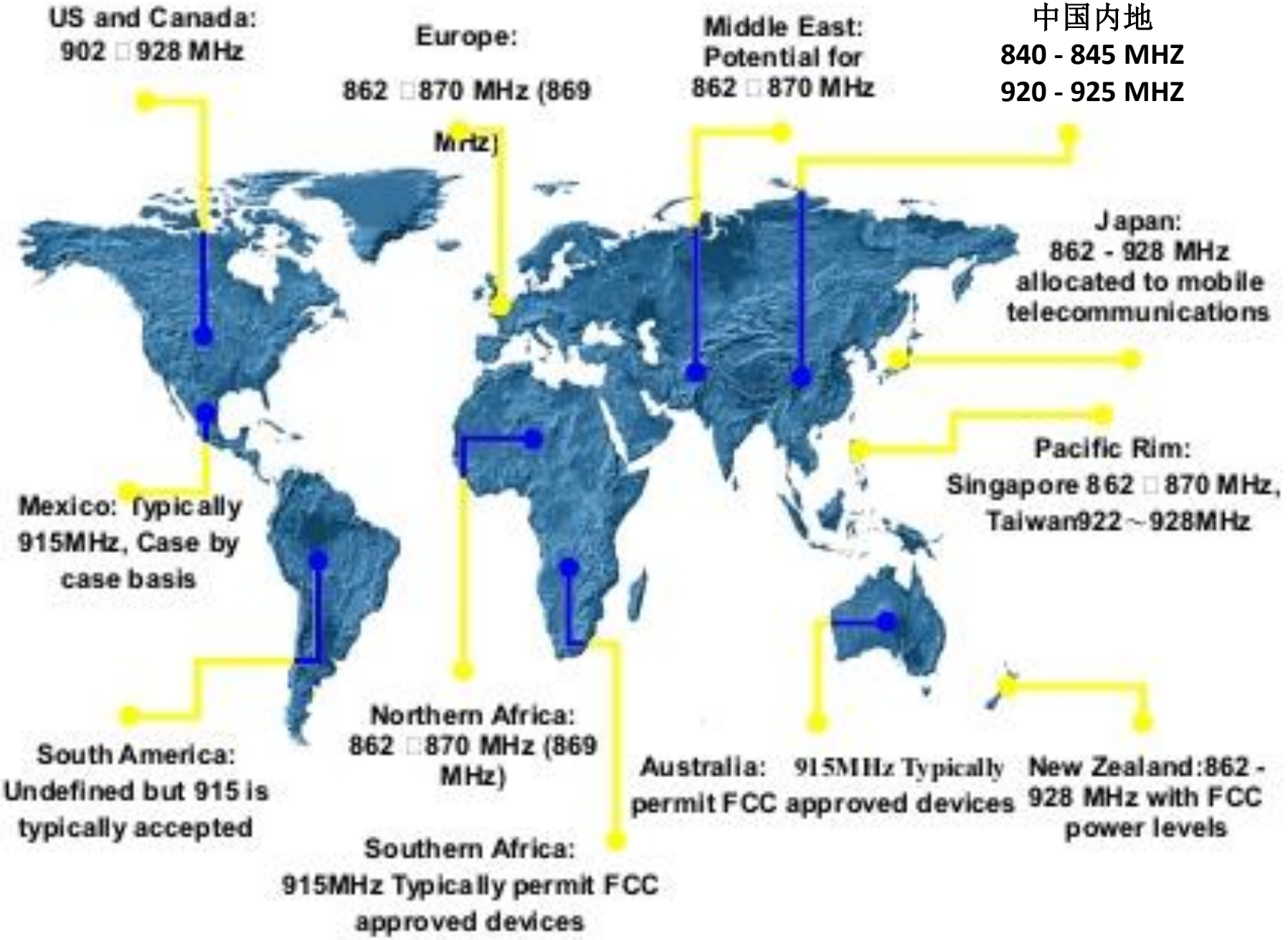
- 读写器发送无线信号时所使用的频率被称为无线射频识别系统的工作频率
  - 低频（30～300kHz）
  - 高频（3～30MHz）
  - 超高频（300MHz～3GHz）
  - 微波（2.45G以上）

工作频率


915 MHz
125 KHz
13.56 MHz
物品管理
交通管理
2.45 GHz
门禁管理
动物识别
智能卡
智能货架
物品管理
交通管理
无线局域网
数据终端
手机
TV
无线电
玩具
调幅广播
调频
广播
车库
10 kHz
100 kHz
1 MHz
10 MHz
100 MHz
1000 MHz
2.45 GHz
300 GHz
频谱

系统工作频率与应用范围

- 射频识别系统属于无线电的应用范畴，因此其使用不能干扰到其他系统的正常工作
- 无线电产品的生产和使用都必须符合国家许可，我国由国家无线电管理委员会进行管理
- 通常情况下，无线射频使用的频段是工业、科学和医疗使用的频率范围（ISM），属于局部的无线电通信频段
- 对于135kHz以下的低频频段可以自由使用射频识别系统

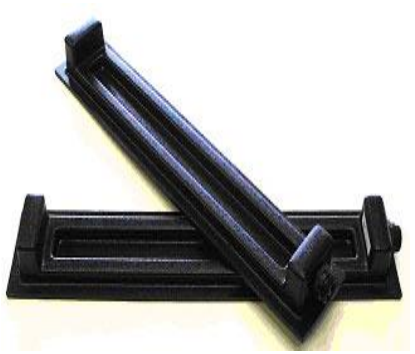

US and Canada:
902 □ 928 MHz
Europe:
862 □ 870 MHz (869 MHz)
Middle East:
Potential for
862 □ 870 MHz
中国内地
840 - 845 MHZ
920 - 925 MHZ
Japan:
862 - 928 MHz
allocated to mobile
telecommunications
Pacific Rim:
Singapore 862 □ 870 MHz,
Taiwan922～928MHz
Mexico: Typically
915MHz, Case by
case basis
South America:
Undefined but 915 is
typically accepted
Northern Africa:
862 □ 870 MHz (869
MHz)
Southern Africa:
915MHz Typically permit FCC
approved devices
Australia: 915MHz Typically
permit FCC approved devices
New Zealand:862 -
928 MHz with FCC
power levels

读写器及天线

读写器及天线

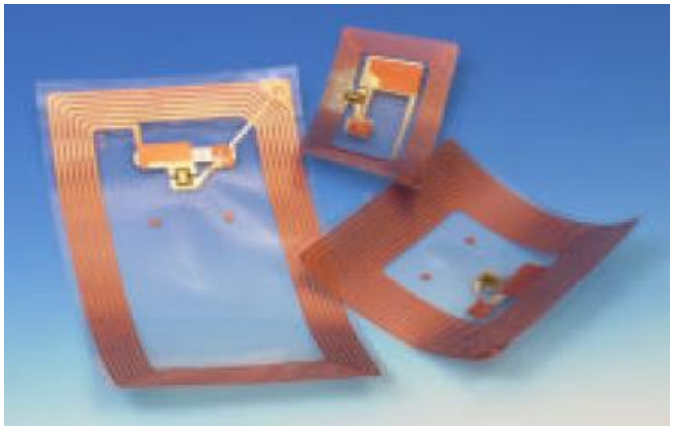
读写器及天线

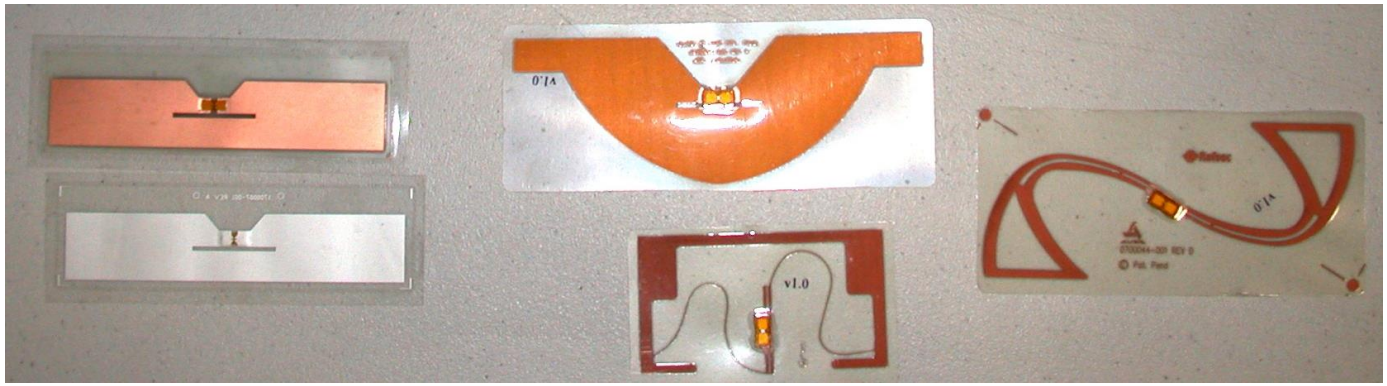
不同的电子标签及封装



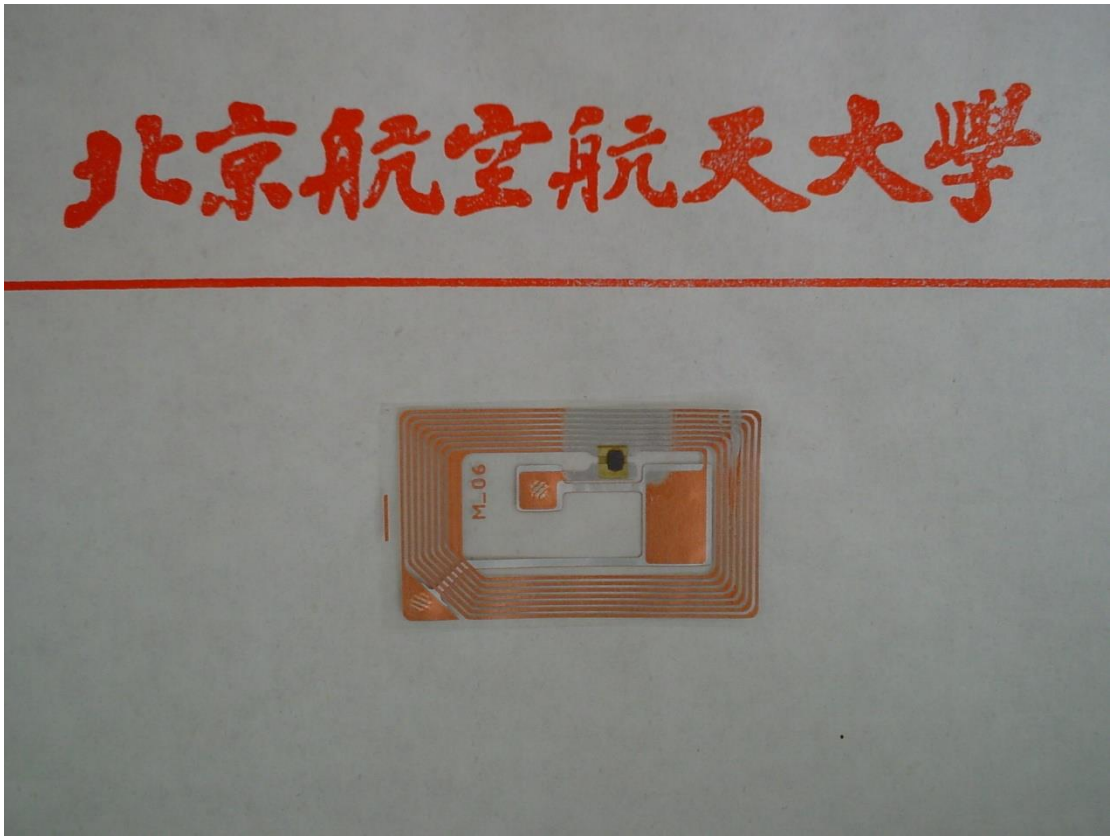
不同的电子标签及封装

- inlay



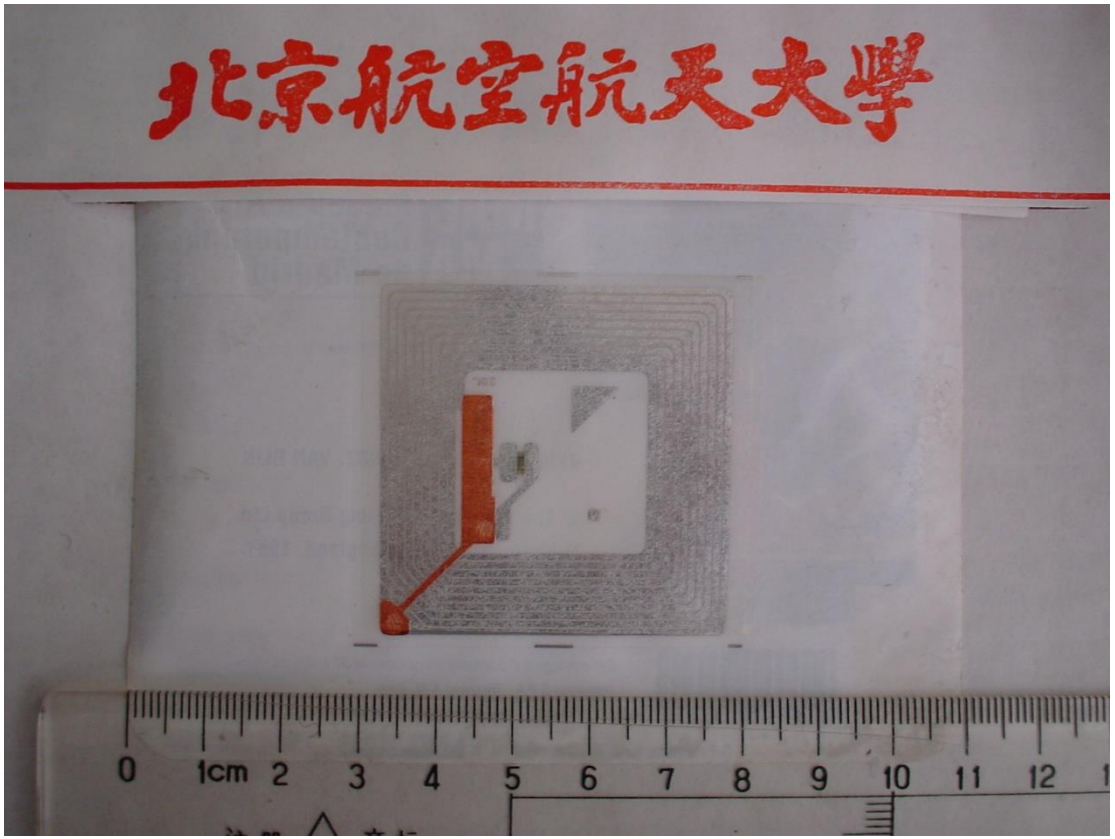


不同的电子标签及封装

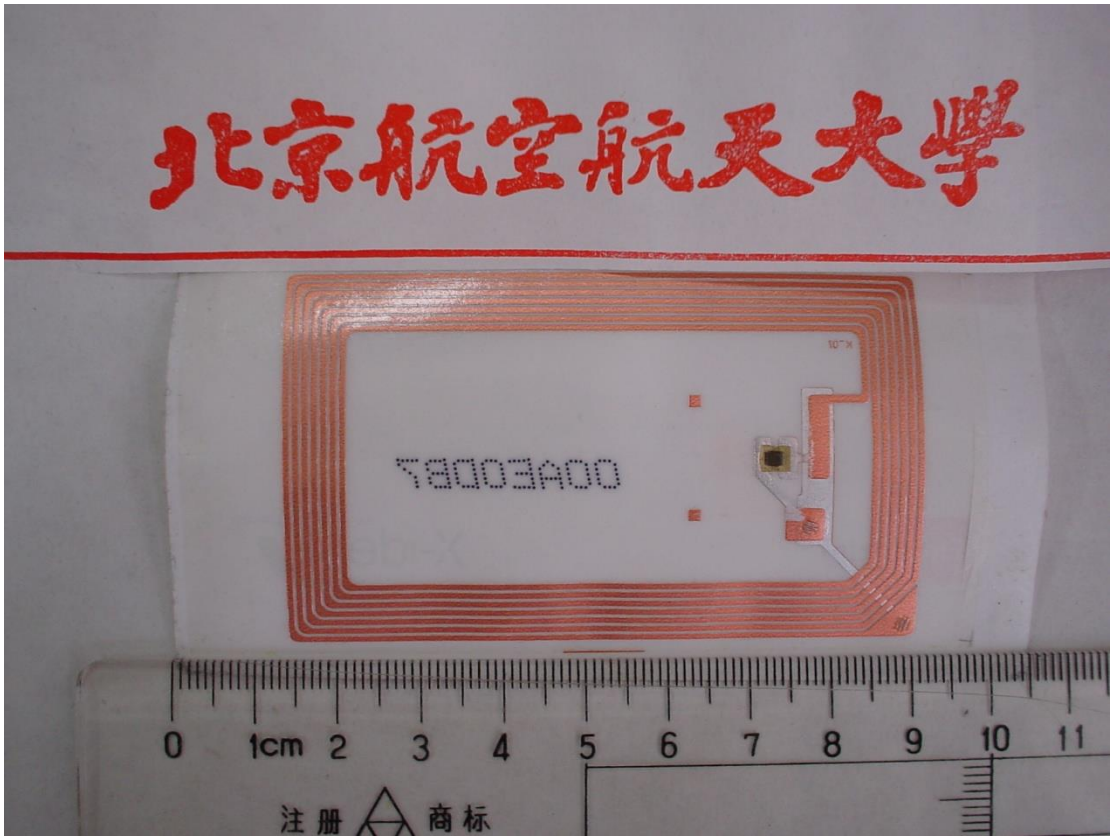


不同的电子标签及封装

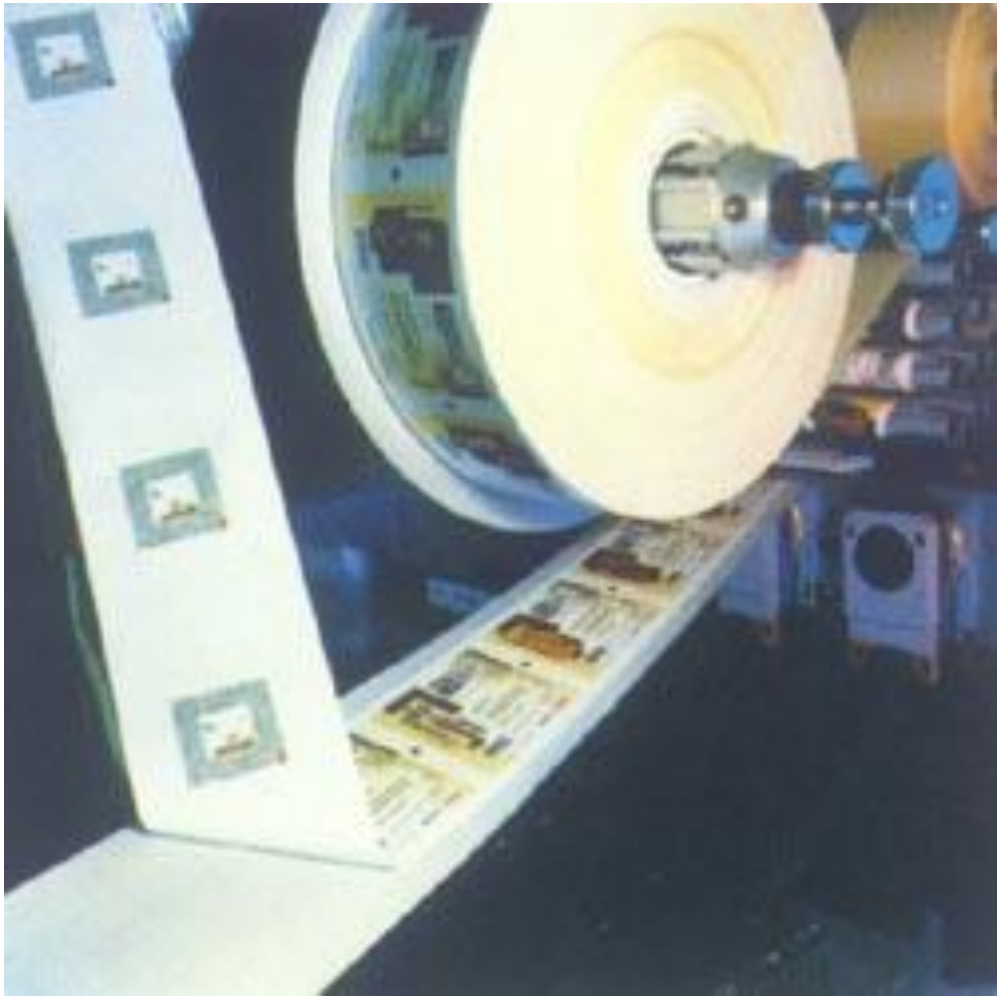
不同的电子标签及封装



不同的电子标签及封装



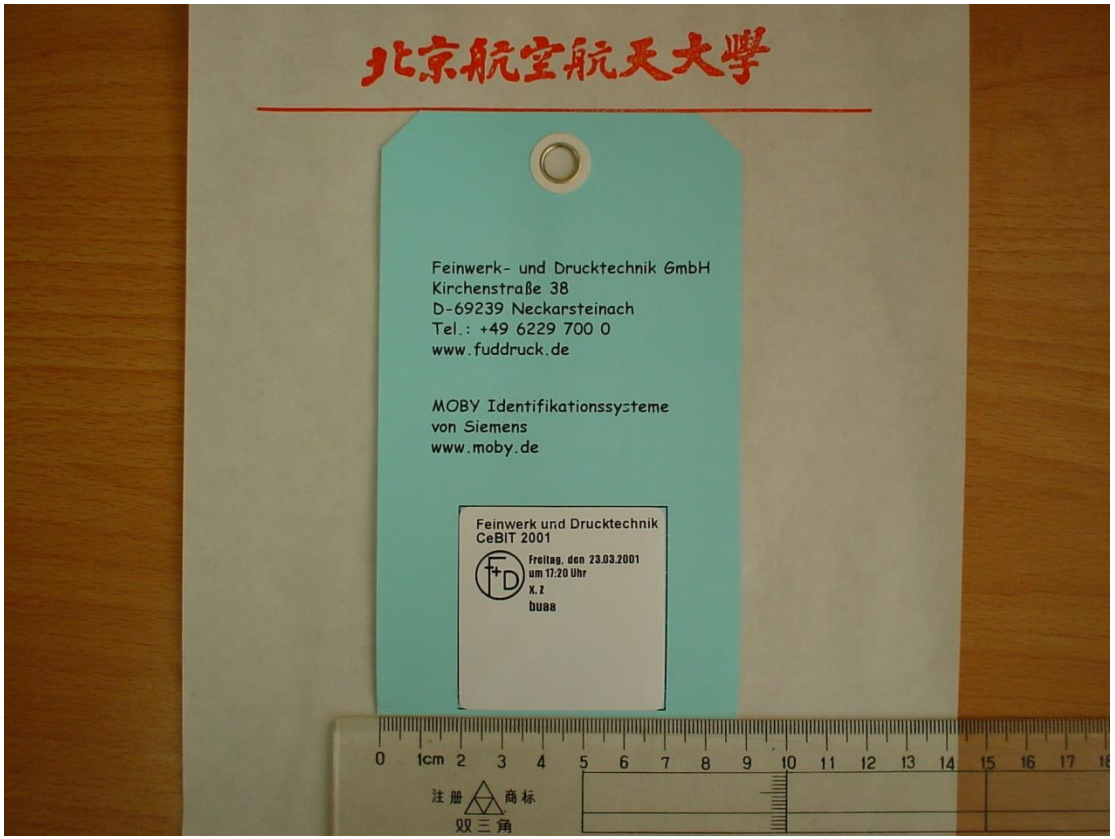
不同的电子标签及封装



不同的电子标签及封装


北京航空航天大學
FROM:
Schreiner Datenträger und Codedruck
Waldvögeleinstraße 12
D – 80995 München
+ 49 (0) 89 15816 – 0
schreiner
TO:
Fachgebiet Logistik
Prof. Dr. – Ing. R. R. Jansen
Leonhard – Euler – Str. 5
D – 44227 Dortmund
FLog
(40) SHIP TO POST
(40)752
PO NUMBER: 238 963 45
ORDER TYPE: RTX
ITEM#: 064 – 640633 – 1
(00) SERIAL SHIPPING CONTAINER:
(00)75243543 000 1
one of our integrated technologies using Philips I – Code
schreiner RFID-Label
phone: +49 (0) 89 1 58 16 – 0
e – mail: rfid@schreiner – etiketten.de web: www.schreiner – etiketten.de
printed on Zebra R140 Smart Label Printer
from Zebra Technologies

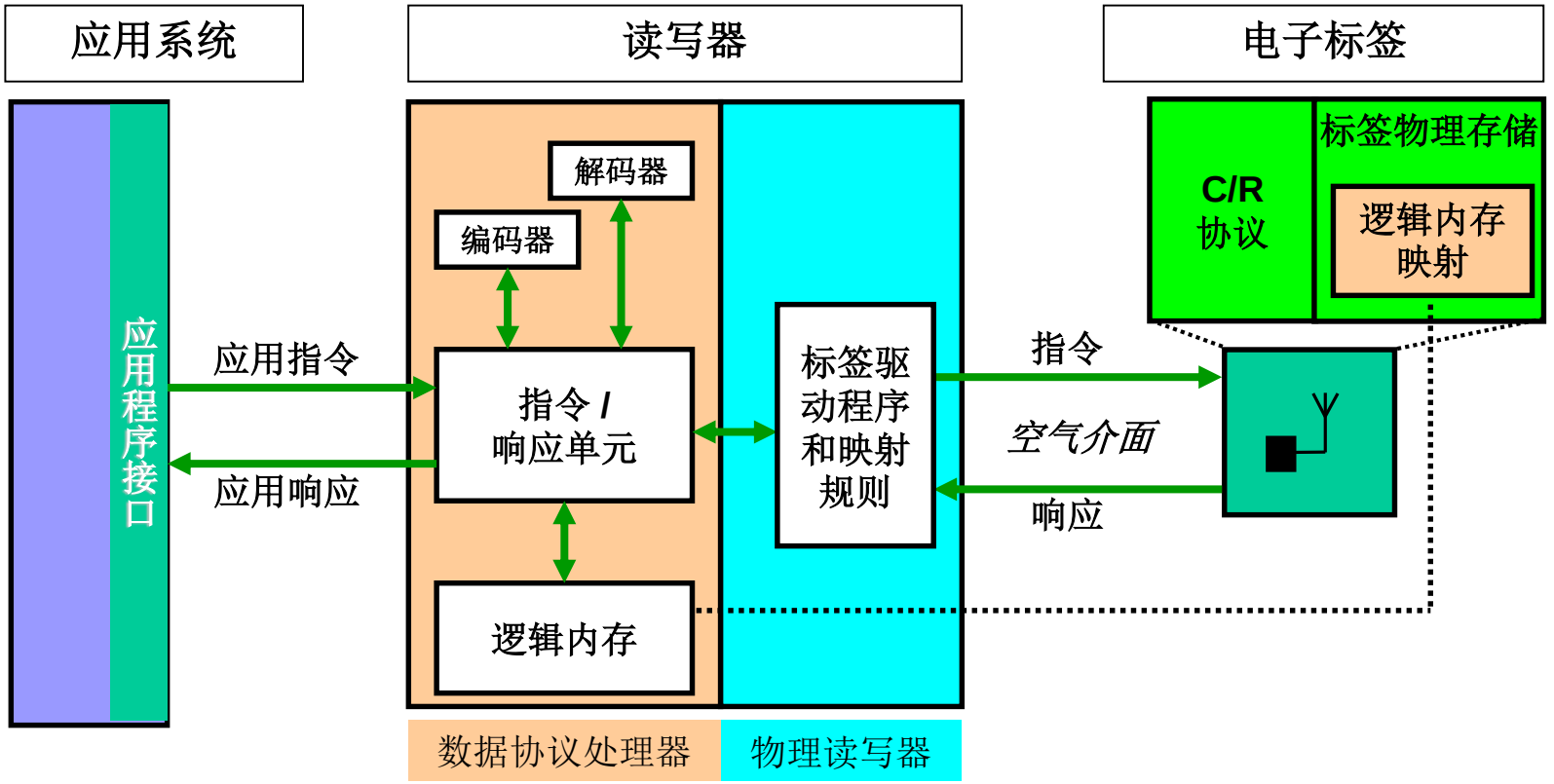
不同的电子标签及封装


北京航空航天大學
Feinwerk- und Drucktechnik GmbH
Kirchenstraße 38
D-69239 Neckarsteinach
Tel.: +49 6229 700 0
www.fuddruck.de
MOBY Identifikationssysteme
von Siemens
www.moby.de
Feinwerk und Drucktechnik
CeBIT 2001
Freitag, den 23.03.2001
um 17:20 Uhr
X. z
buaa
0 1cm 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
注册 商标
双三角

不同的电子标签及封装

不同的电子标签及封装

无线射频识别系统工作原理



读写器的主要功能

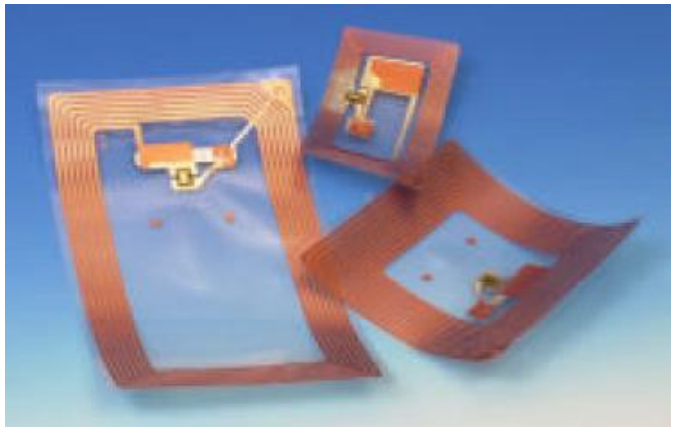
- 与应答器的通信功能：读写器的基本功能
- 与应用系统之间的通信功能：让应用系统能够对读写器进行控制并处理应答器的数据信息
- 在读写区内实现多应答器识别，完成防冲突功能
- 校验读写过程中的错误

读写器与应用系统之间的接口

- 应用系统→读写器
  - 配置命令
  - 其他命令
- 读写器→应用系统
  - 当前配置状态
  - 命令的执行结果

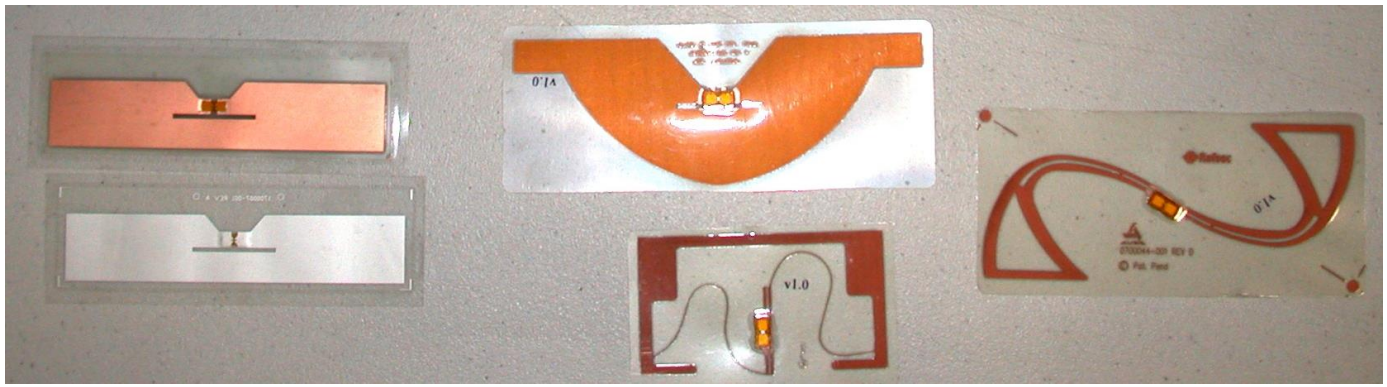
发生在读写器和标签之间的射频信号的耦合类型有两种

- 电感耦合
  - 变压器模型、电磁感应定律
  - 典型作用距离为10～20cm
  - 典型工作频率125kHz, 225kHz, 13.56MHz
  - 具有环形天线的典型低频、高频标签

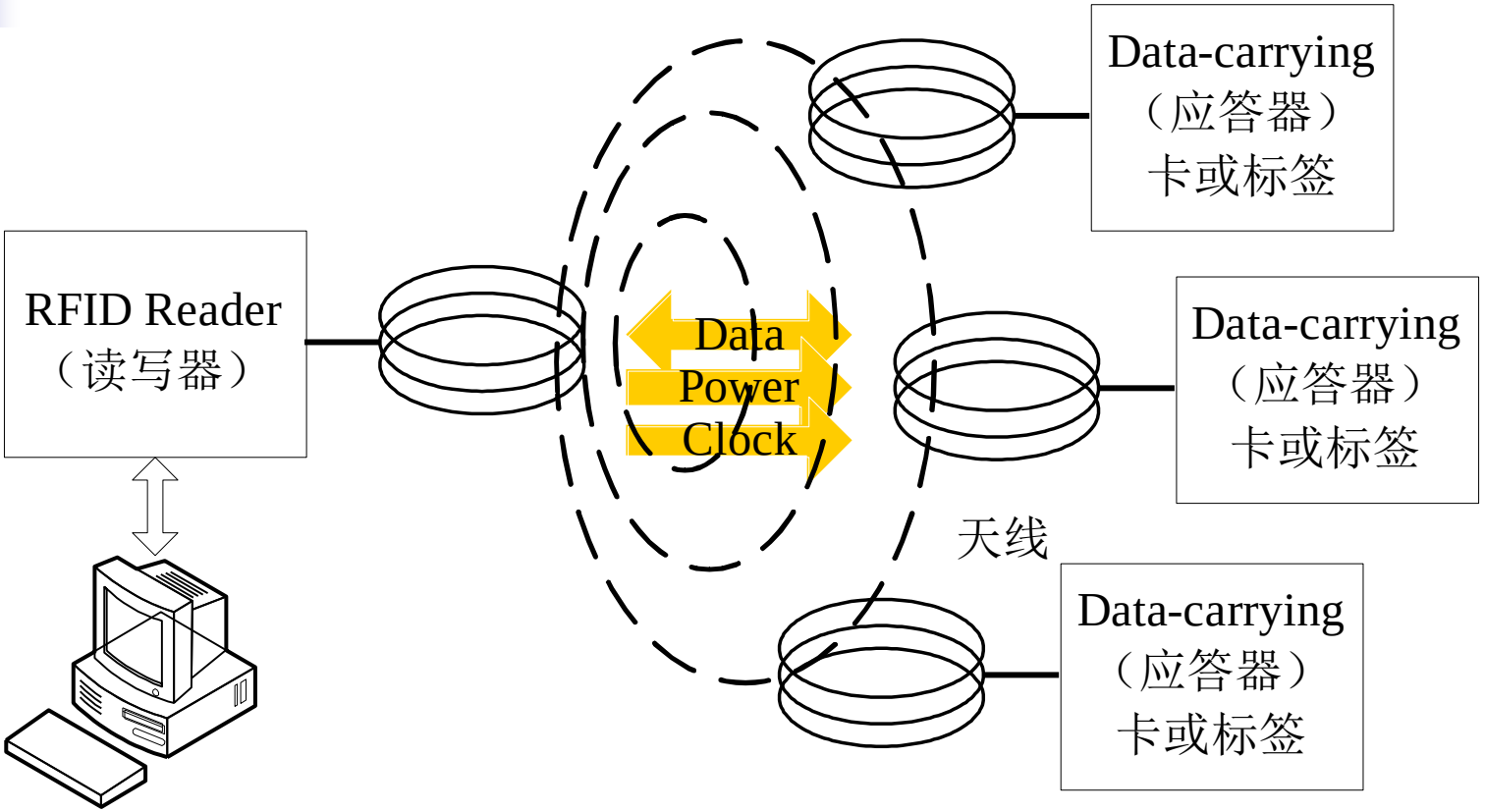


发生在读写器和标签之间的射频信号的耦合类型有两种

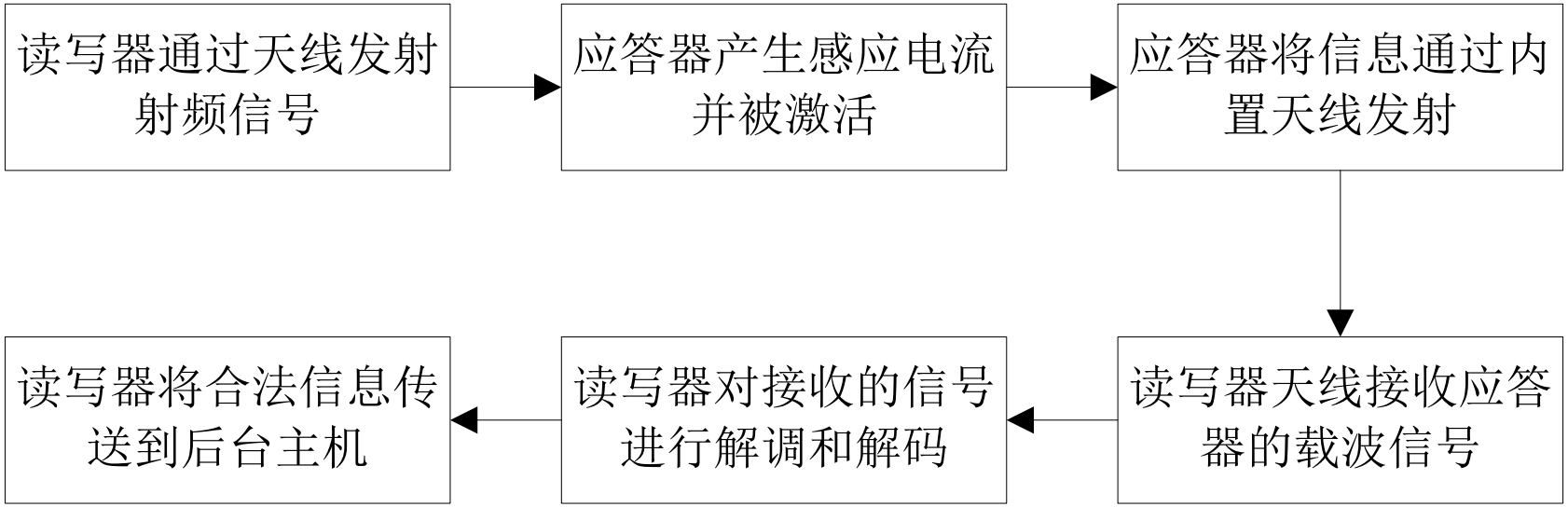
- 电磁反向散射耦合
  - 雷达原理模型、电磁波的空间传播规律
  - 典型工作距离为3～10m
  - 典型工作频率为433MHz,915MHz,2.45GHz,5.8GHz
  - 具有双极天线的超高频和微波标签



无线射频识别系统的基本构成



被动式标签系统流程图


读写器通过天线发射射频信号
应答器产生感应电流并被激活
应答器将信息通过内置天线发射
读写器天线接收应答器的载波信号
读写器对接收的信号进行解调和解码
读写器将合法信息传送到后台主机

工作时序方式

- 读写器和电子标签的工作次序
  - 读写器先讲（Reader Talk First, RTF）
  - 标签先讲（Tag Talk First, TTF）
- 多标签同时识读（无冲突）

数据通信方式

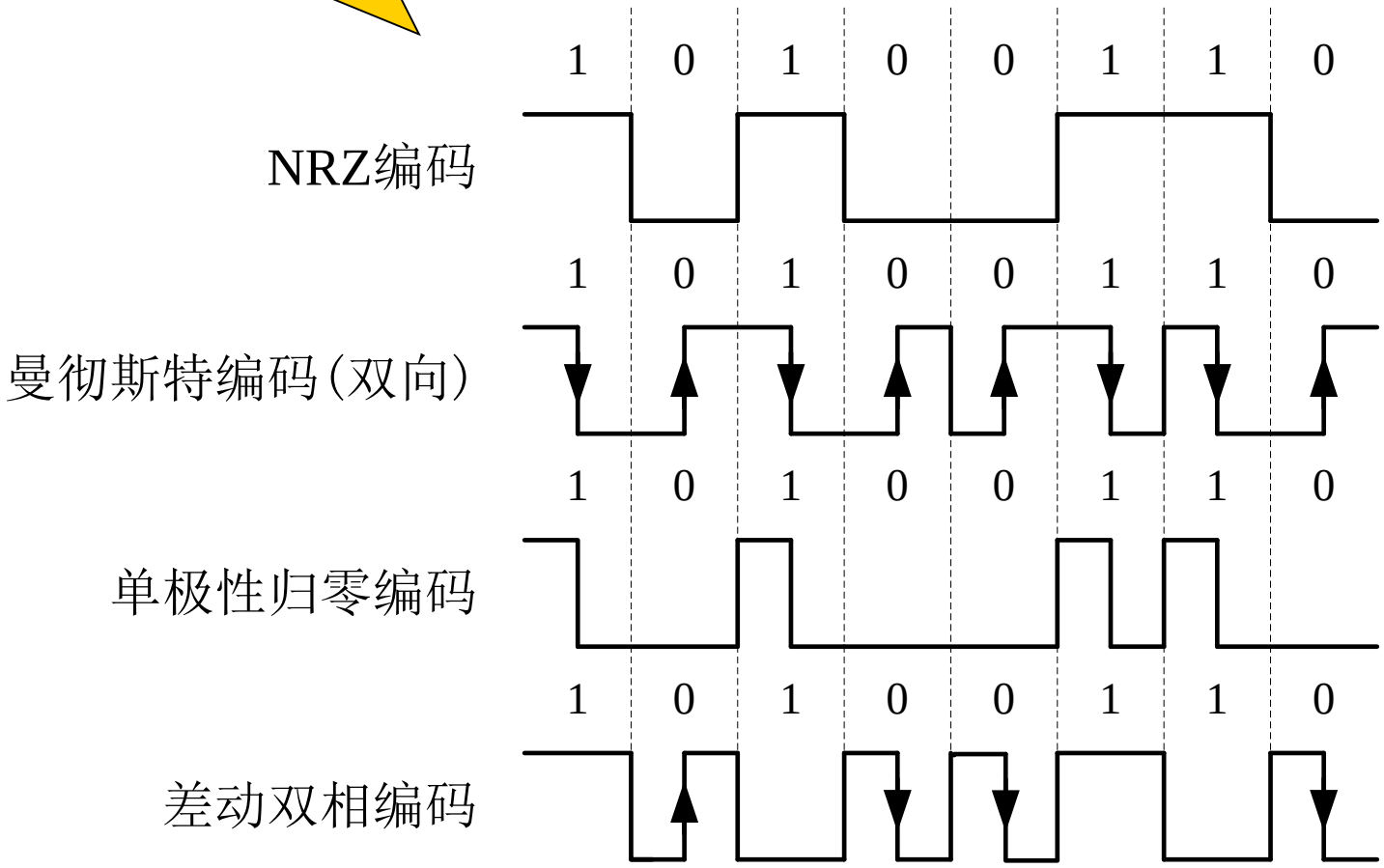
- 读写器→标签
  - 数据写入（离线/在线）
- 标签→读写器
  - 标签收到读写器的射频能量时，即被激活并向读写器反射标签存储的数据信息
  - 标签被激活后，根据读写器的指令转入数据发送状态或休眠状态

数据编码方法

- 反向不归零码（Non Return to Zero）
- 曼彻斯特编码（Manchester）
- 单极性归零编码（Unipolar RZ）
- 差动双相编码（DBP）
- 米勒编码（Miller）
- 差动编码（Differential）
- 脉冲宽度编码（Pulse Width Modulation）
- 脉冲位置编码（Pulse Position Modulation）

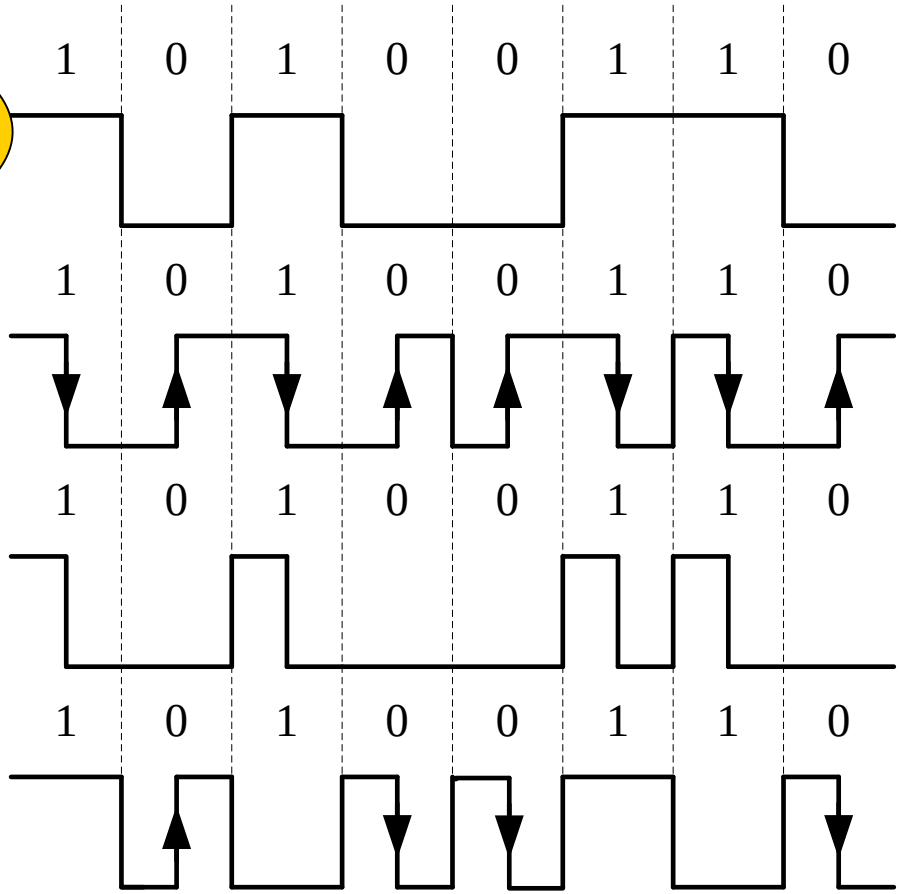
方法

“高”电平表示1
“低”电平表示0

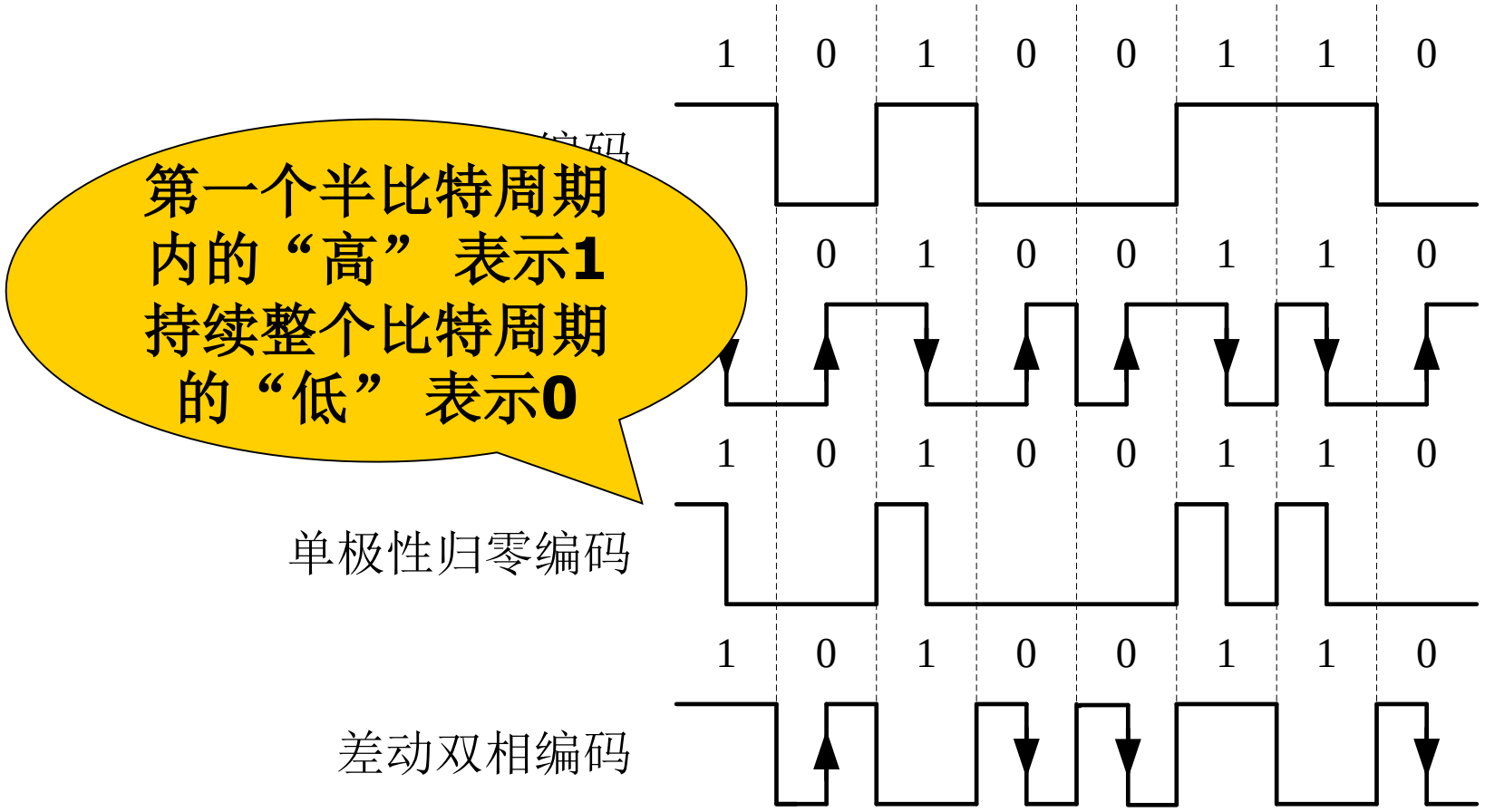


数据编码方法

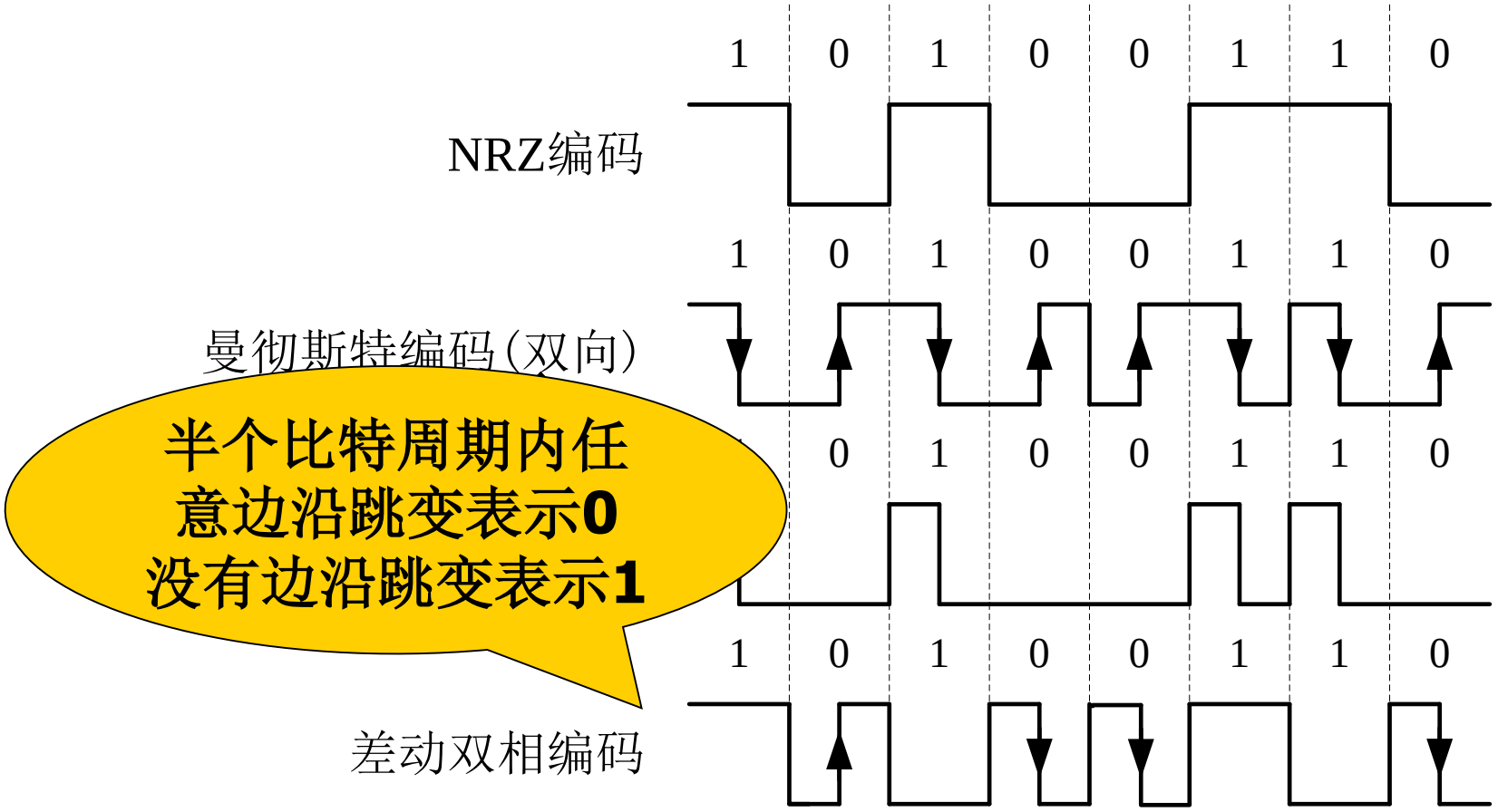
半个比特周期时的负跳变表示1
正跳变表示0



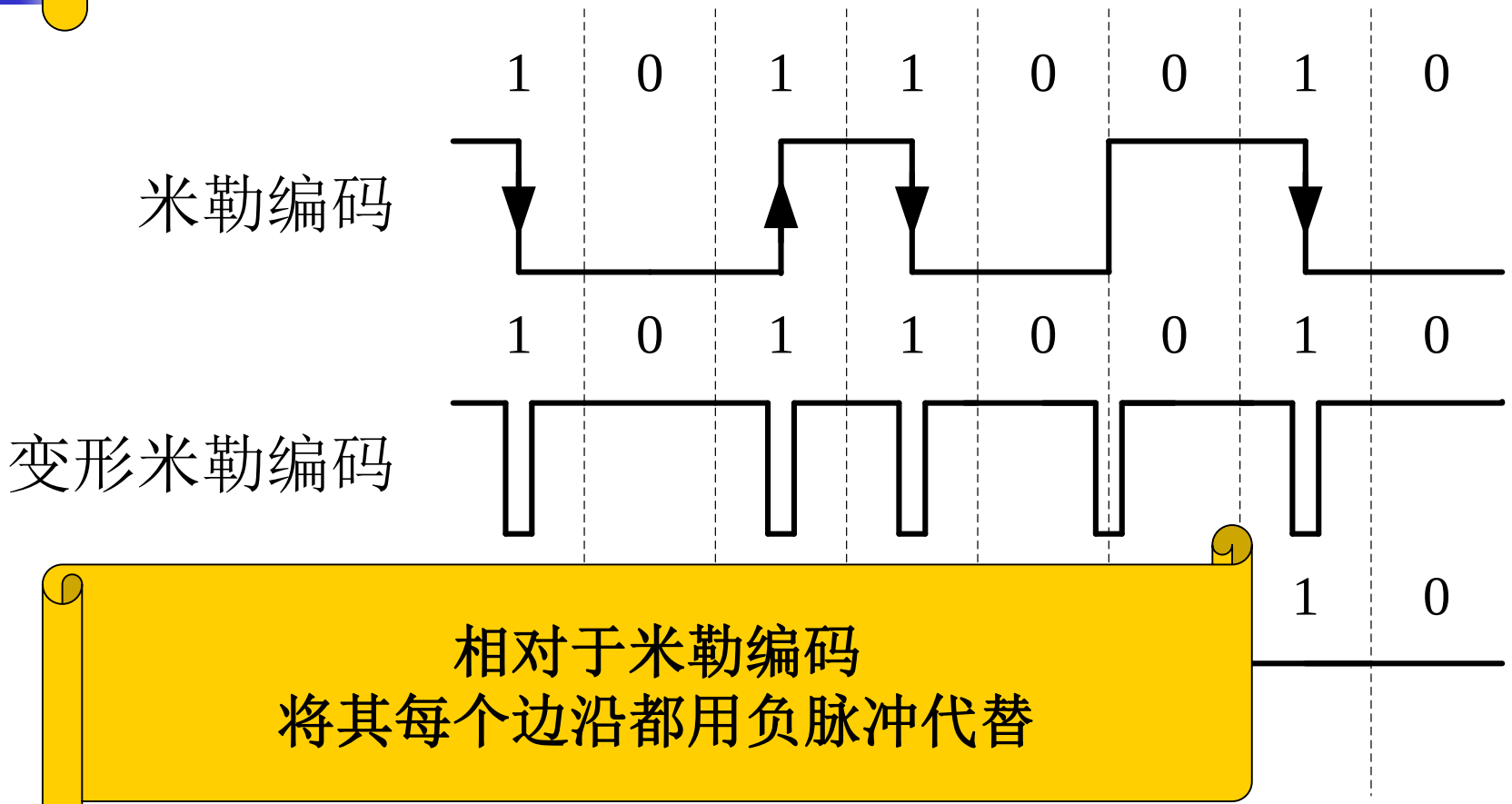
数据编码方法


1 0 1 0 0 1 1 0
第一个半比特周期内的“高” 表示1
持续整个比特周期的“低” 表示0
1 0 1 0 0 1 1 0
单极性归零编码
1 0 1 0 0 1 1 0
差动双相编码

数据编码方法

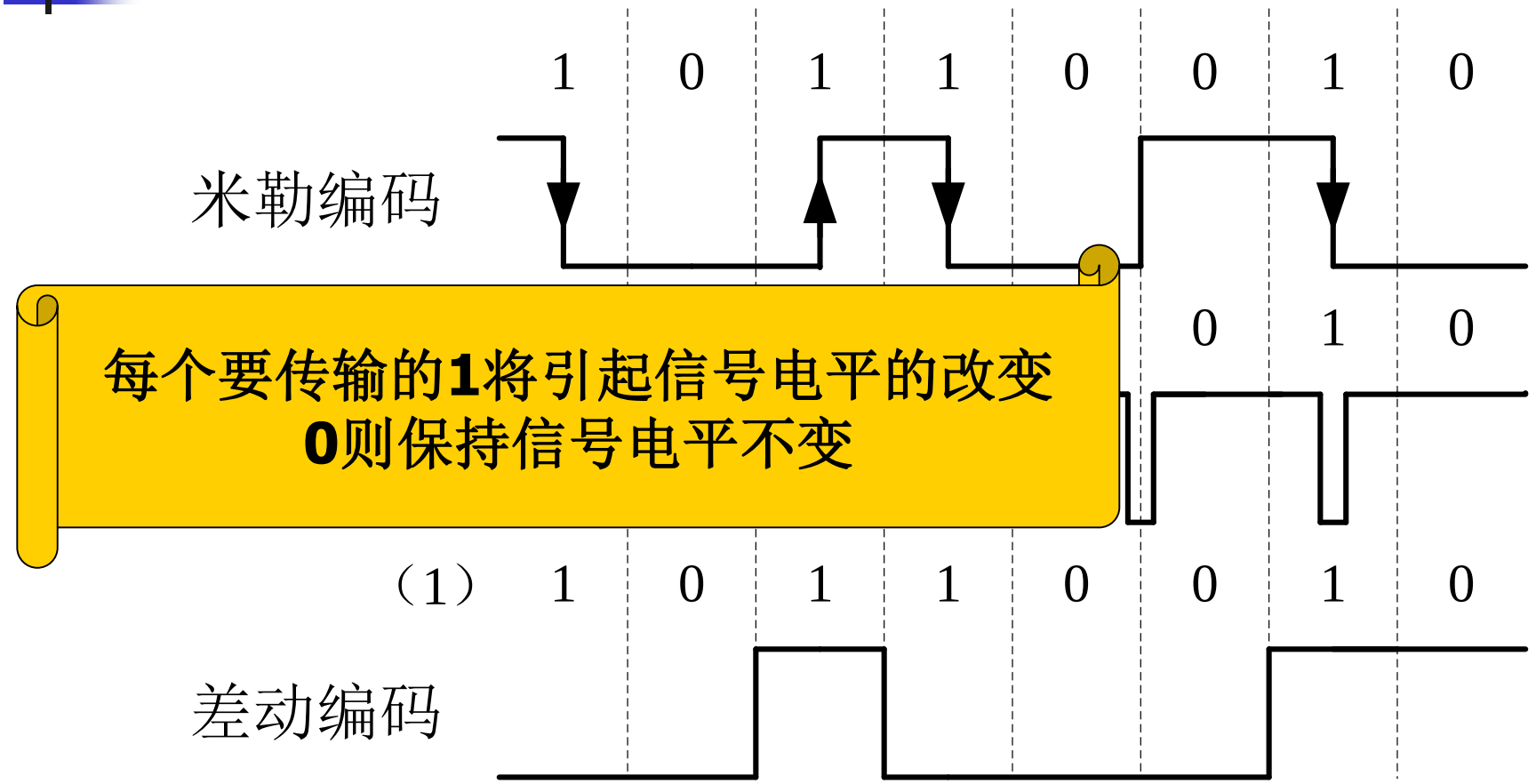

1 0 1 0 0 1 1 0
NRZ编码
1 0 1 0 0 1 1 0
曼彻斯特编码(双向)
半个比特周期内任意边沿跳变表示0
没有边沿跳变表示1
0 1 0 0 1 1 0
1 0 1 0 0 1 1 0
差动双相编码

半个比特周期内的任意边沿跳变表示1
经过下一个比特周期不变的1电平表示0
连续的0在比特周期开始的时产生跳变



相对于米勒编码
将其每个边沿都用负脉冲代替

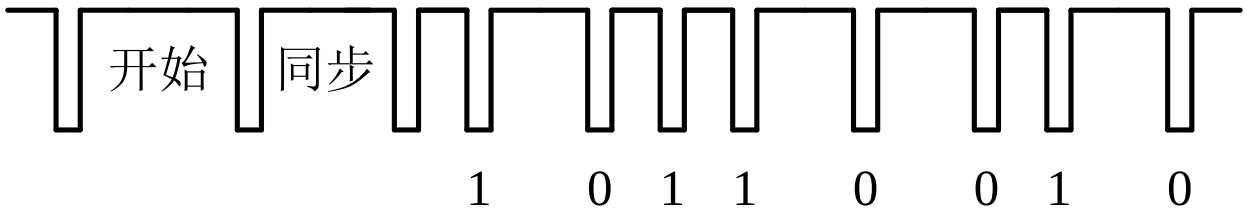
数据编码方法


1 0 1 1 0 0 1 0
米勒编码
每个要传输的1将引起信号电平的改变
0则保持信号电平不变
0 1 0
（1） 1 0 1 1 0 0 1 0
差动编码

数据编码方法

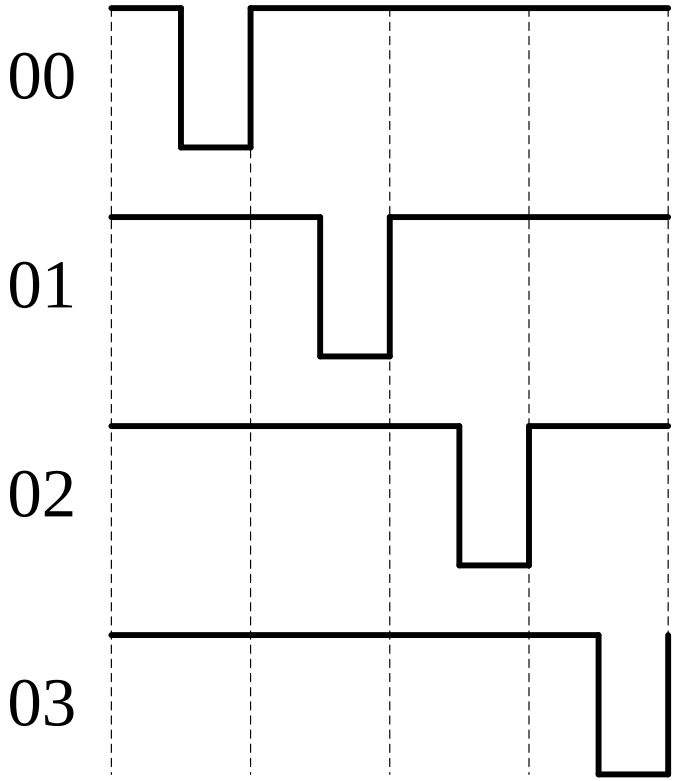
在下一脉冲前的暂停持续时间t表示1
下一脉冲前的暂停持续时间2t表示0
“开始”和“同步”也是用不同间隔t的脉冲来表示的

脉冲-间歇编码



数据编码方法--脉冲位置编码

- 每个数据比特的宽度是一致的
- 脉冲出现在
  - 第一个时间段表示00
  - 第二个时间段表示01
  - 第三个时间段表示10
  - 第四个时间段表示11



作业

- 将学号按位以十进制相加，得到一个两位数，将其想象成两位16进制数，画出其八种数据编码方式波形示意图
- 如33060332，3+3+0+6+0+3+3+2 = 20，则画出00100000的示意图
- 生成jpg或者pdf，画笔、visio绘图均可，不建议手绘拍照
- 上传至课程中心course.buaa.edu.cn

数据编码方法

- 反向不归零码（Non Return to Zero）
- 曼彻斯特编码（Manchester）
- 单极性归零编码（Unipolar RZ）
- 差动双相编码（DBP）
- 米勒编码（Miller）
- 差动编码（Differential）
- 脉冲宽度编码（Pulse Width Modulation）
- 脉冲位置编码（Pulse Position Modulation）

数据安全性

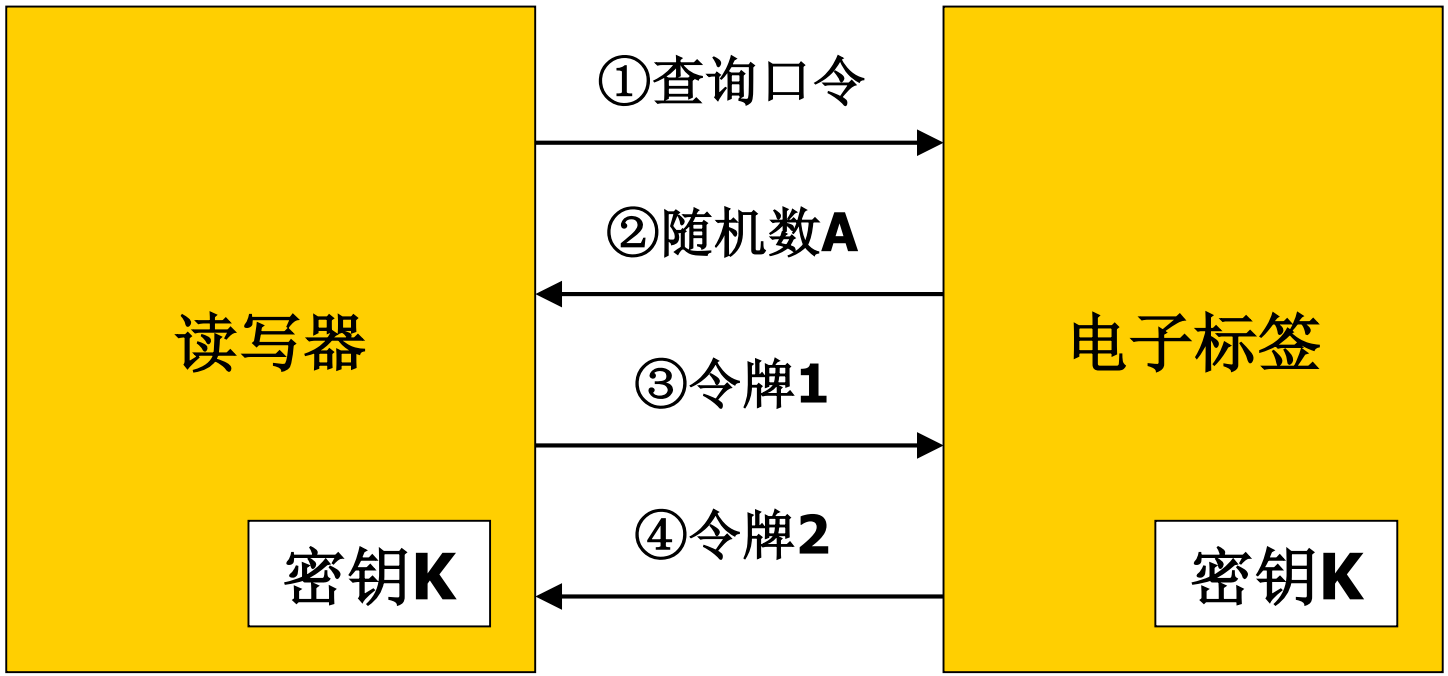
- 高度安全的射频识别系统对于以下单项攻击应能够予以防范
  - 为了复制或改变数据，未经授权的读取数据载体
  - 将外来的数据载体置入某个读写器的询问范围内，企图进行一些非授权的行为
  - 为了假冒真正的数据载体，窃听无线电通信并重放数据

相互对称的鉴别

- 加密密钥和解密密钥一样

- 读写器：需要防止假冒的伪造数据
- 标签：需要防止未经认可的数据读取或重写

相互对称的鉴别过程



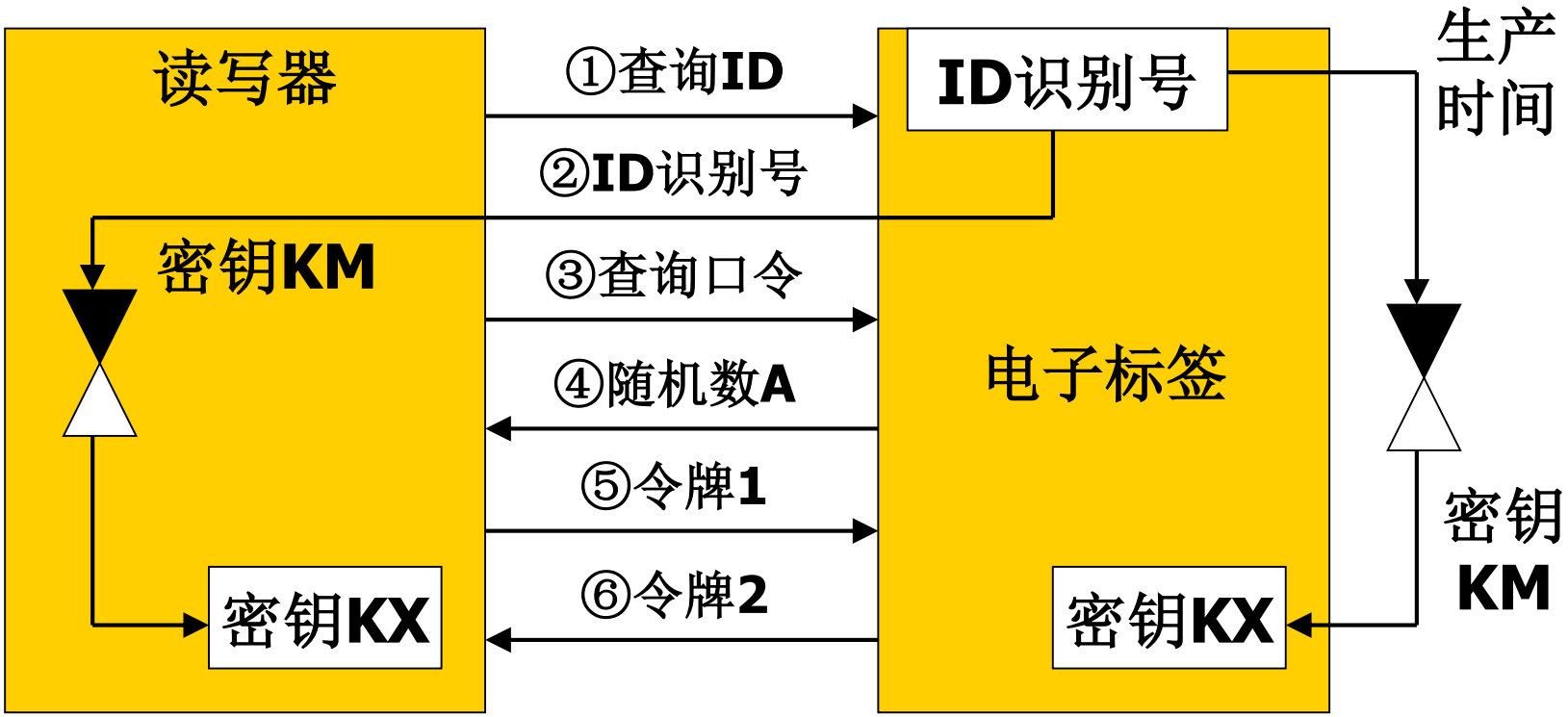
相互鉴别过程的优点

- 密钥从不经过空间传输，而只是传输加密的随机数
- 总是两个随机数同时加密，排除了为了计算密钥用随机数A执行逆变换获取令牌1的可能性
- 可以使用任意算法对令牌进行加密
- 通过严格使用来自两个独立源（标签、读写器）的随机数，使回放攻击而记录鉴别序列的方法失败
- 从产生的随机数可以算出随机的密钥，以便加密后续传输的数据

相互鉴别过程的缺点

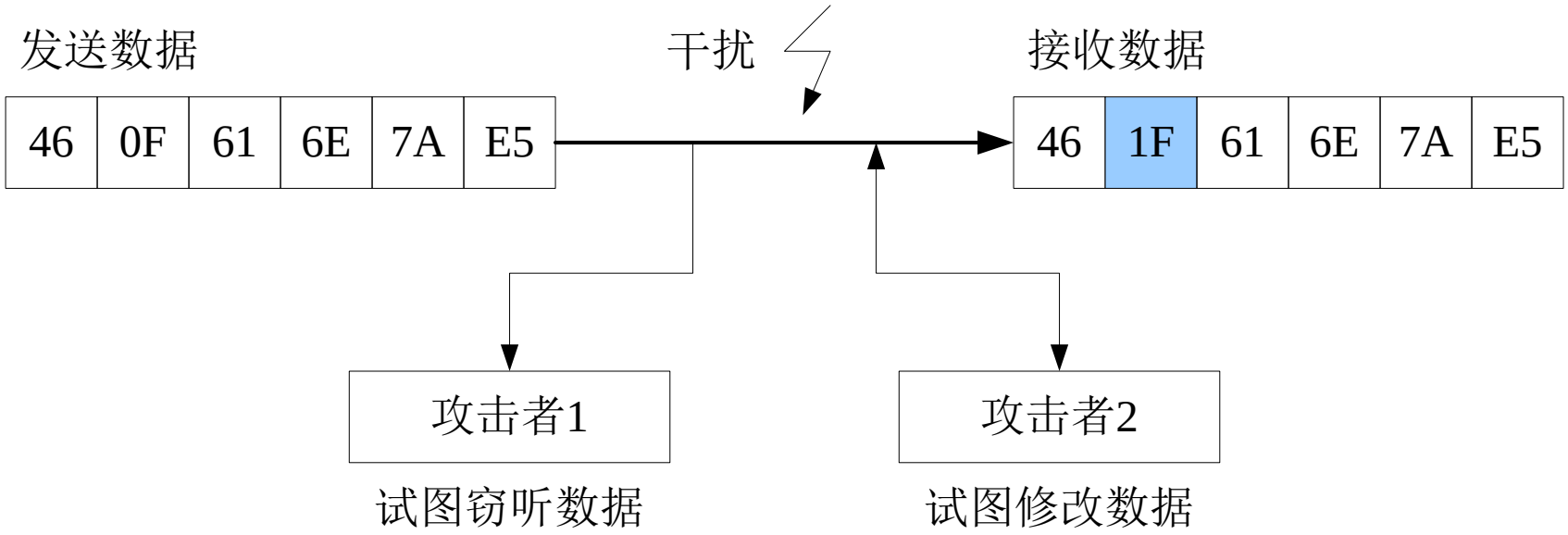
- 所有属于同一应用的标签都采用相同的密钥K来保护
- 安全程度依赖于密钥的保密程度

改进后的相互对称的鉴别过程——利用导出密钥的鉴别



加密的数据传输

- 数据在传输时受到的物理影响可能是面临某种干扰（隐藏的攻击者）



加密算法

- 对称加密算法：加密密钥和解密密钥相同，或者相互间有直接的关系
- 非对称加密算法：解密过程与加密密钥的知识无关

- 序列密码：每个符号在传输前单独加密
- 分组密码：多个符号划分为一组进行加密

数据完整性

- 采用非接触技术传输数据时，很容易遇上干扰，使传输数据发生改变，因而导致传输错误，通常采用数据检错与纠错算法来解决

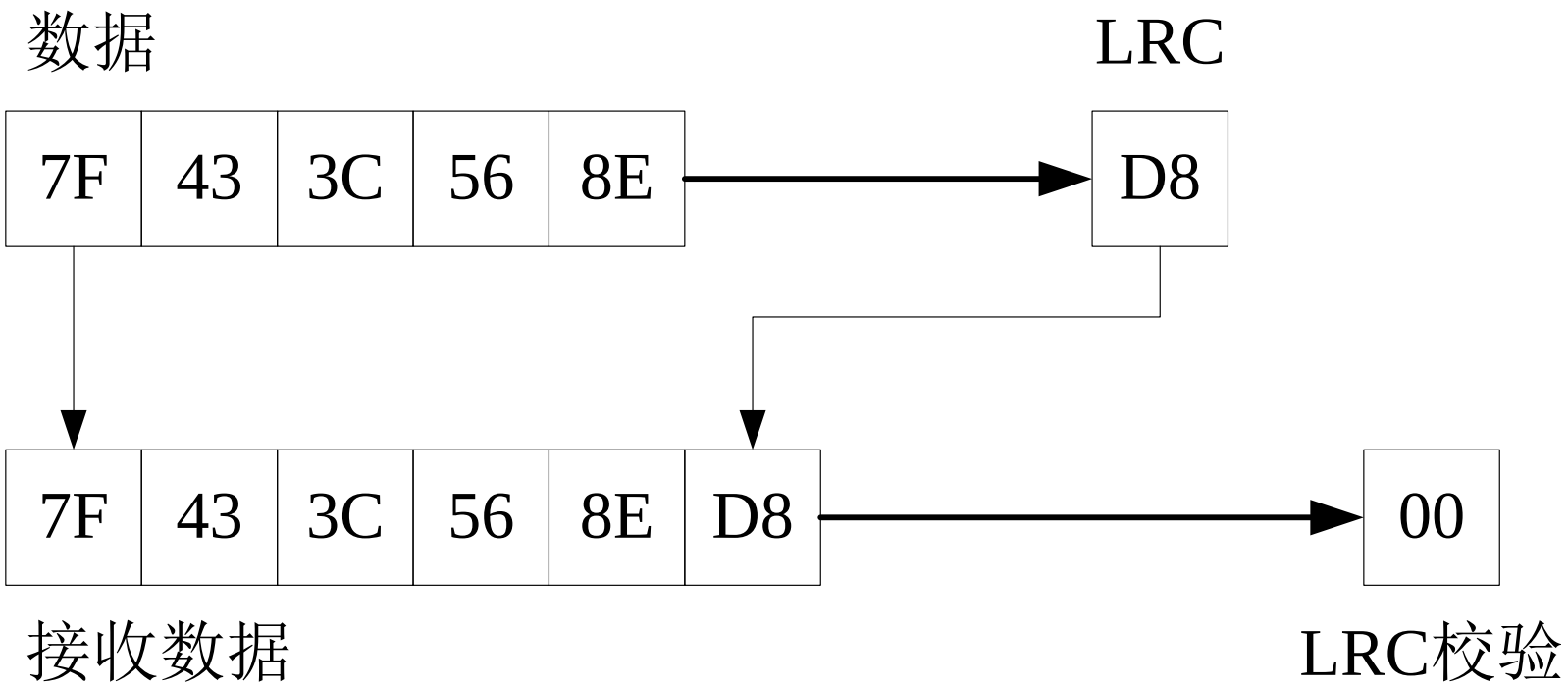
- 常采用的方法有奇偶校验、纵向冗余校验（LRC）、循环冗余校验（CRC）

奇偶校验法

- 把一个奇偶校验位组合到每一字节中（即每字节发送9位）
- 接收端对接收到的数据进行与发送端相同的校验方法

- 优点：简单，且广泛使用
- 缺点：识别错误的能力低

纵向冗余校验法（LRC）

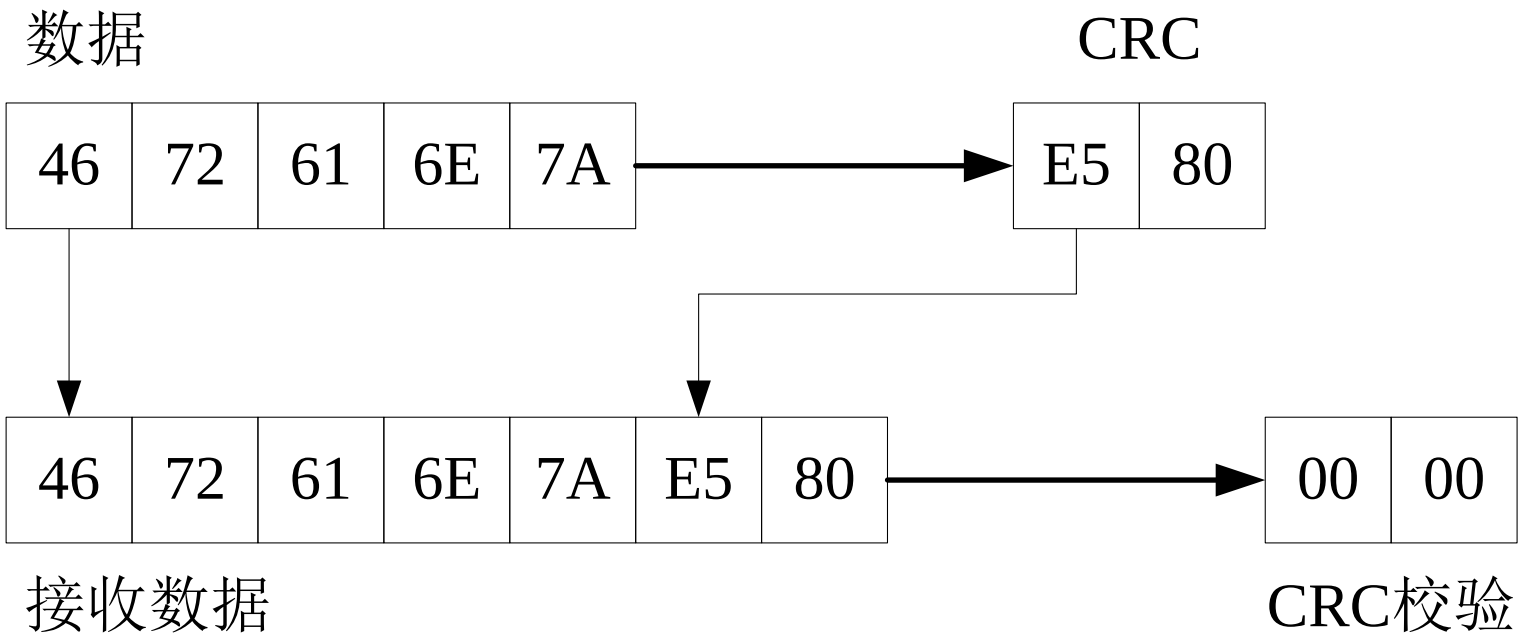


纵向冗余校验法（LRC）

- 优点：算法简单
- 缺点：多个错误可能相互抵消

- 主要用于快速校验很小的数据块
- 对容量较小的标签（每次交互数据量不大）比较适合

循环冗余校验法（CRC）



循环冗余校验法（CRC）

- 以8位数据91H（10010001）为例
- 可把它看成是7次多项式
  M（x）＝x^7+x^4+1的系数
- 算法规则（CRC码）为4次多项式
  G（x）＝x^4+x^2+1，系数为10101
- 在信息码后面添加4个0
  构成多项式$x^4 \cdot M(x)$即100100010000

循环冗余校验法（CRC）

```
                10110111
          ┌──────────
10101 ／  100100010000
          10101
          ─────
           11100
           10101
           ─────
            10011
            10101
            ─────
             11000
             10101
             ─────
              11010
              10101
              ─────
               11110
               10101
               ─────
                1011
```

```
                10110111
          ┌──────────
10101 ／  100100011011
          10101
          ─────
           11100
           10101
           ─────
            10011
            10101
            ─────
             11010
             10101
             ─────
              11111
              10101
              ─────
               10101
               10101
               ─────
                   0
```

常用的CRC码

- $G(x) = x^8+x^2+x+1$
- $G(x) = x^{12}+x^{11}+x^3+x^2+x+1$
- $G(x) = x^{16}+x^{12}+x^5+1$ （CCITT）
- $G(x) = x^{16}+x^{12}+x^2+1$ （IBM）
- $G(x) = x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$

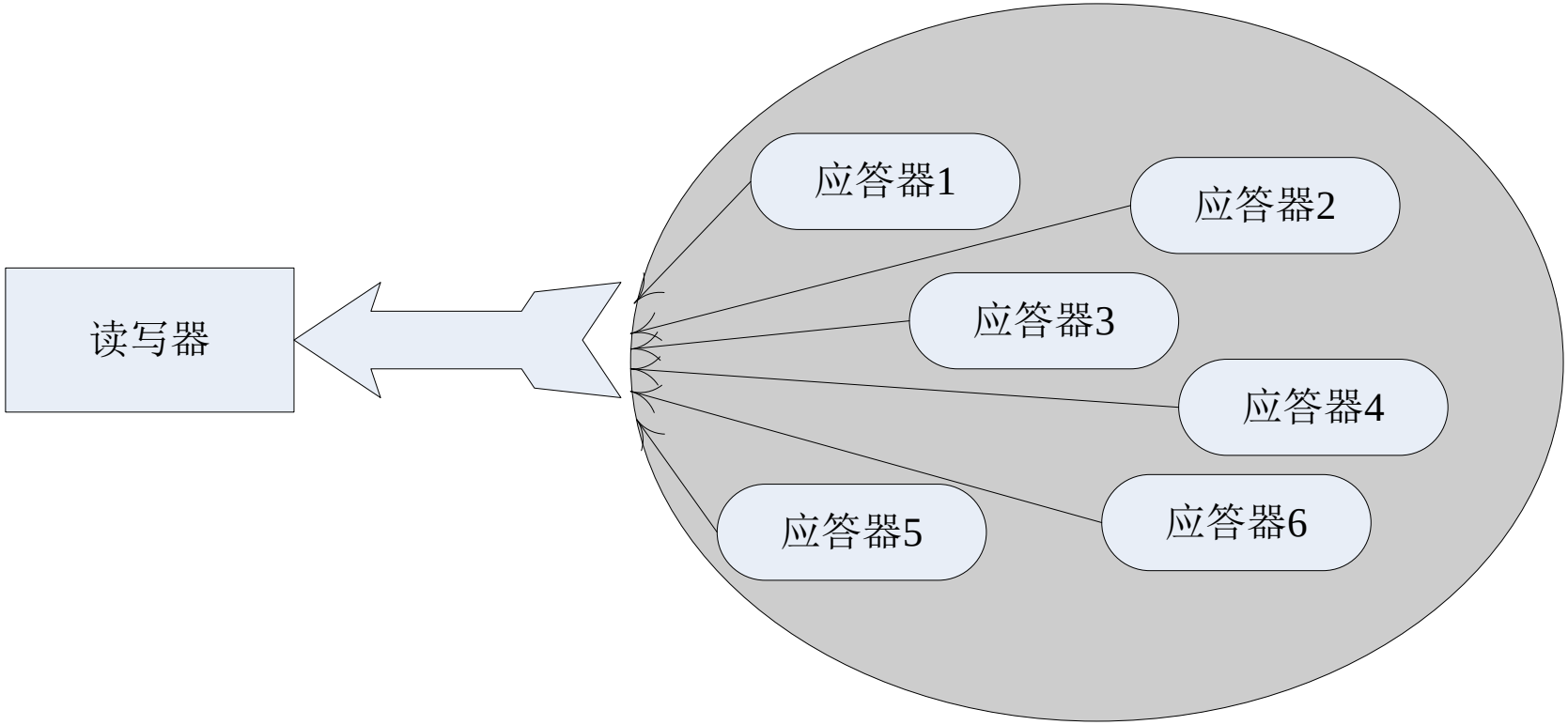
干扰与抗干扰

- 标签
  - 标签错误的响应读写器的命令
  - 标签工作状态的混乱
  - 可写入标签错误的进入休眠状态
- 读写器
  - 不能识别正常工作的标签，误判标签故障
  - 将一个标签判别为另外一个标签，造成识别错误

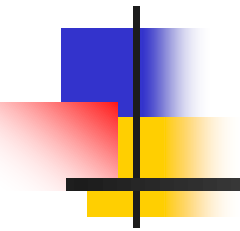
可能的抗干扰措施

- 通过标签与读写器通信约定的数据完整性方法，检验出受到干扰出错的数据
- 通过数据编码提高数据传输过程中的抗干扰能力，使得数据传输中不容易受到干扰
- 通过数据编码与数据完整性校验，纠正数据传输中的某些差错
- 通过多次重发、比较剔除出错的数据并保留判断为正确的数据

多目标识别与系统防冲突




LAWSON
秒拍
胡椒视频



谢谢！