移动互联网技术及应用

第三章
移动互联网的终端

计算机学院
段鹏瑞

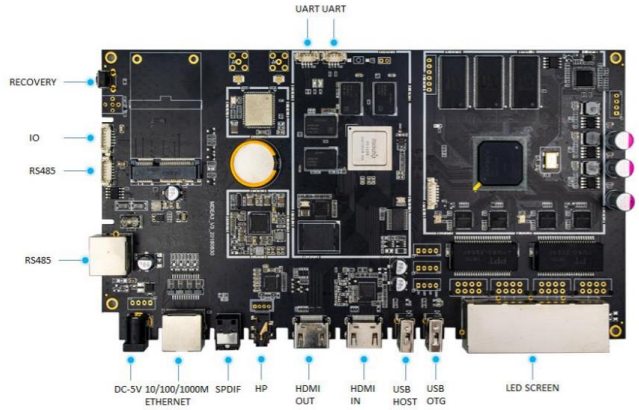
本章内容

- 移动互联网络的各种终端
- 自动识别技术
  - NFC
  - RFID
  - 二维码

终端…

- 智能手机
- 笔记本电脑
- 共享单车、ETC终端
- 智能手表、手环
- 无线传感网节点
- 列车车厢
- 运动服、球鞋
- 手持POS机、自动售货机、人脸识别门禁、收银机、汽车多媒体、电子班牌、快递柜、影院取票机、广告视频机
- 它们应用在不同场景，具备不同的联网能力

工控开发板的应用



开发板

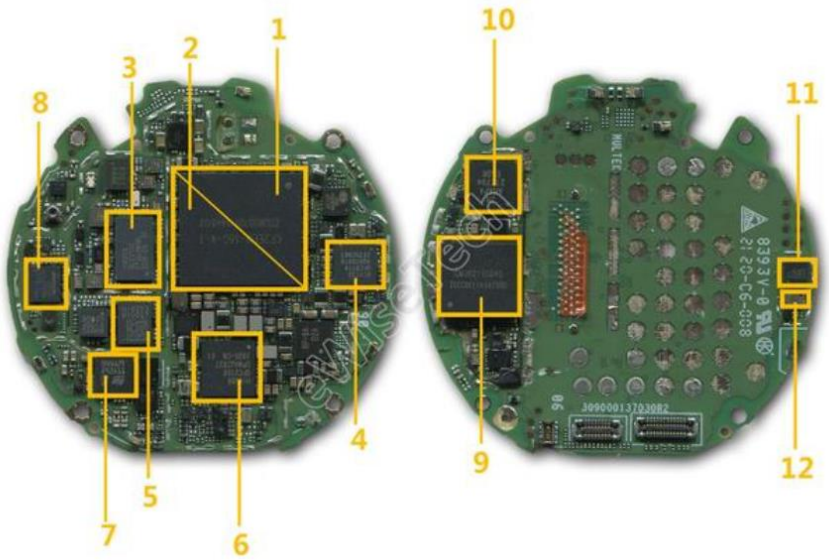
技术参数

CPU	PX30，四核Cortex-A35，MALI-G31 MP2
内存/存储	1GB/ 16GB
MIPI LCD	支持 1080P@60Hz 输出
触摸屏	支持多点电容触摸屏
视频格式支持	支持 wmv、avi、flv、rm、rmvb、mpeg 、ts、mp4 等
图片格式支持	支持 BMP、JPEG、PNG、GIF
音频接口	支持左右声道输出，支持MIC录音
USB2.0 接口	1 个 USB OTG、2 个 USB HOST
WIFI、BT	内置 WIFI，BT4.0（标配）
扩展接口	支持2路UART，1路USB，8路GPIO
RTC 实时时钟	支持定时开关机
电源	Mirco USB 5V输入， 支持7.4V电池
板卡尺寸	110.4mm*64mm
系统升级	Android8.1(标配)，支持Linux系统

智能手表

- 铝合金外壳配备 1.78" Super AMOLED 屏幕
- （Snapdragon） Wear 3100 平台
- 1 GB RAM 和 8 GB 存储空间
- 扬声器和用于打电话的麦克风（通过 e-SIM）
- 计步器，睡眠监测，光学心率传感器
- Wi-Fi，GPS，NFC 还有 Bluetooth

华为WATCH 3



1：Hisilicon-Hi8262-处理器
2：16GB闪存
3：Hisilicon-Hi6D05-功率放大器模块
4：Hisilicon-Hi1132-麒麟A1芯片
5：Hisilicon - Hi6353 -射频收发器
6：Hisilicon - Hi6556 -电源管理
7：STMicroelectronics - ST54H - NFC控制芯片
8：AIROHA - AG3335MN - GPS 接收器
9：2GB RAM
10：Ambiq Micro-AMA3B1KK-KBR-超低功耗微控制器
11：STMicroelectronics-6轴加速度计+陀螺仪
12：AKM-AK09918C-电子罗盘

共享单车

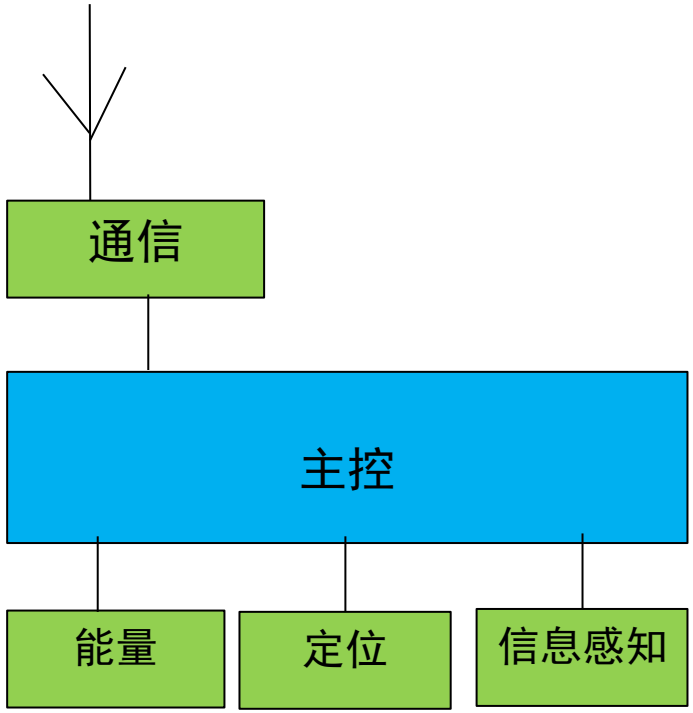
中心控制单元、GPS定位模块、2G移动通信模块、机电锁车装置、电池、动能发电模块、充电管理模块、车载加速度计等。

- ✓ 短信开锁，GSM 模块
- ✓ GPRS开锁，GPRS/3G模块
- ✓ 蓝牙解锁，短距连接
- ✓ LTE IoT开锁，eMTC/NB-IoT模块

北京郵電大學
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

终端的模块组成

- 主控模块、通信模块、能量模块、定位模块、信息感知模块等

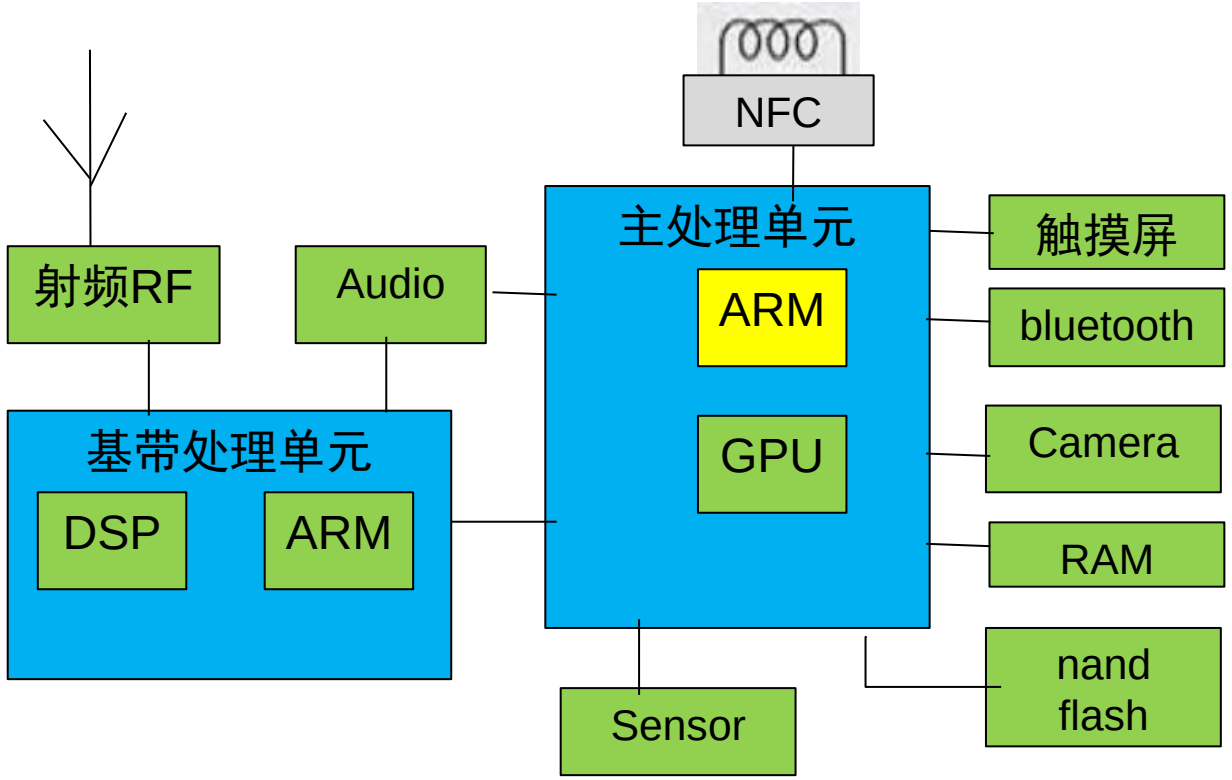


智能手机的组成

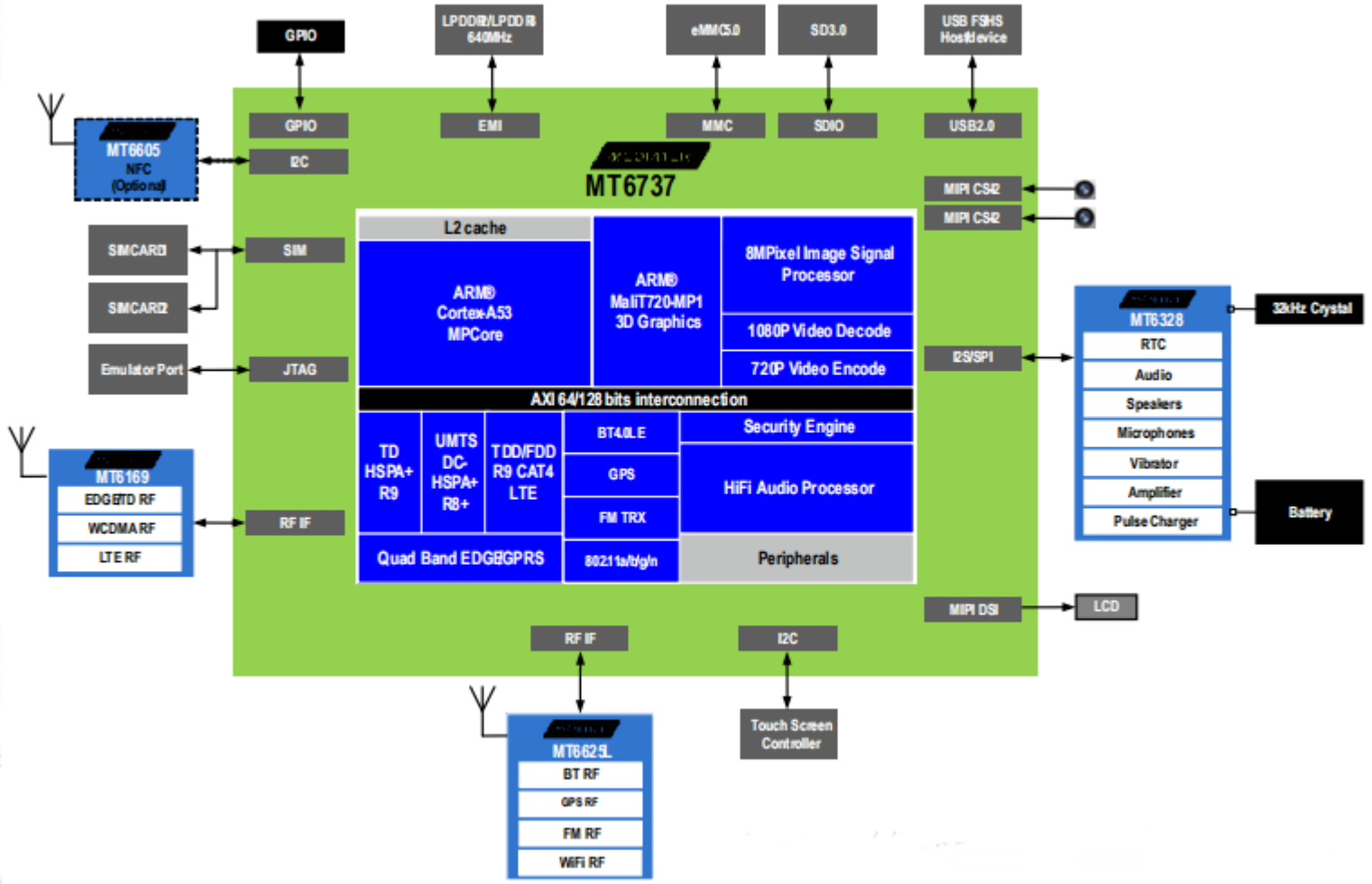
- 由主处理单元、基带处理单元、射频处理单元、天线、GPU、存储单元、音频、视频、触摸屏、液晶显示、传感器等组成

智能手机架构

- 主处理单元
  - ARM 多核
    Android 、 iOS
  - GPU
- 基带处理单元
  - DSP： 调制、解调、A/D、D/A
  - ARM： GSM与LTE通信协议栈



手机芯片举例：



移动开发平台

- 华为、高通、三星、联发科、苹果

	Apple A11 Bionic	Huawei Kirin 970	Qualcomm Snapdragon 845	Samsung Exynos 9810
Process	10nm FinFET+ (TSMC)	10nm FinFET+ (TSMC)	10nm FinFET LPP (Samsung)	10nm FinFET LPP (Samsung)
Physical Size	87.66mm2	96.72mm2	91mm2	118.94mm2
CPU	Hexa Core (2x Monsoon @ 2.39GHz + 4x Mistral)	Octa-Core (4x Cortex-A73 @ 2.36GHz + 4x Cortex-A53 @ 1.84GHz)	Octa-Core (4x Kryo 385 Gold @ 2.8GHz + 4x Kryo 385 Silver @ 1.8GHz)	Octa-Core (4x Exynos M3 @ 2.9GHz + 4x Cortex-A55 @ 1.9GHz)
CPU Architecture	ARM v8-A	ARM v8-A	ARM v8-A	ARM v8-A
GPU	Apple-Made Tri-Core GPU	Mali-G72 MP12 (850MHz)	Adreno 630	Mali-G72 MP18 (572MHz)
RAM Compatibility	LP-DDR4X	LP-DDR4X	LP-DDR4X	LP-DDR4X
Storage	NVMe	UFS	UFS	UFS 2.1, SD 3.0
ISP	Custom	Dual-14 bit ISP	Dual-14 Bit Spectra ISP	Dual-ISP
DSP	Custom	Tensilica Vision P6	Hexagon 685	VPU
Radio	Non-Integrated (Intel XMM7480)	LTE Cat. 18, 5CA, 1.2Gbps DL; Cat. 13, 2CA, 150Mbps DL	X20 (LTE Cat. 18, 5CA, 1.2Gbps DL; Cat. 13, 2CA, 150Mbps DL)	Shannon (LTE Cat. 18, 6CA, 1.2Gbps DL; Cat. 18 2CA 200Mbps UL)
AI/ML Cores	Yes (Dual-Core Neural Engine based on Ceva DSP cores)	Yes (Kirin NPU)	Yes (Hexagon 685)	Yes (VPU)

本章内容

- 移动互联网络的各种终端
- 自动识别技术
  - NFC
  - RFID
  - 二维码

NFC技术

- 近场通信（Near Field Communication，简称NFC），是由射频识别（RFID）演变而来的应用技术，它在单一芯片上集成读卡器与标签。
- NFC具有双向连接和识别的特点，NFC的通信距离为10厘米以内，运行频率13.56MHz，传输速度有106Kbit/s、212Kbit/s或者424Kbit/s三种。
- 这项技术最初只是RFID技术和网络技术的简单合并，现在已经演变成一种短距离无线通信技术。NFC技术在ISO 18092、ECMA 340和ETSI TS 102 190框架下推动标准化，同时也兼容应用广泛的ISO 14443 Type-A、B等非接触式智能卡。

NFC应用模式

- 卡模式
  - 该模式就是将具有NFC功能的设备模拟成一个RFID的Tag标签，如门禁卡、银行卡等。卡模拟模式主要用于商场、交通等非接触移动支付应用中
- 读卡器式
  - NFC设备作为RFID读卡器使用，在该模式中，具备读写功能的NFC手机可从RFID的Tag中采集数据，然后根据应用的要求进行处理， 比如从海报或者展览信息电子标签上读取相关信息
- 点对点式
  - 即将两个具备NFC功能的设备链接，实现点对点数据传输。基于该模式，多个具有NFC功能的数字相机、PDA 计算机、手机之间，都可以进行无线互联，实现数据交换

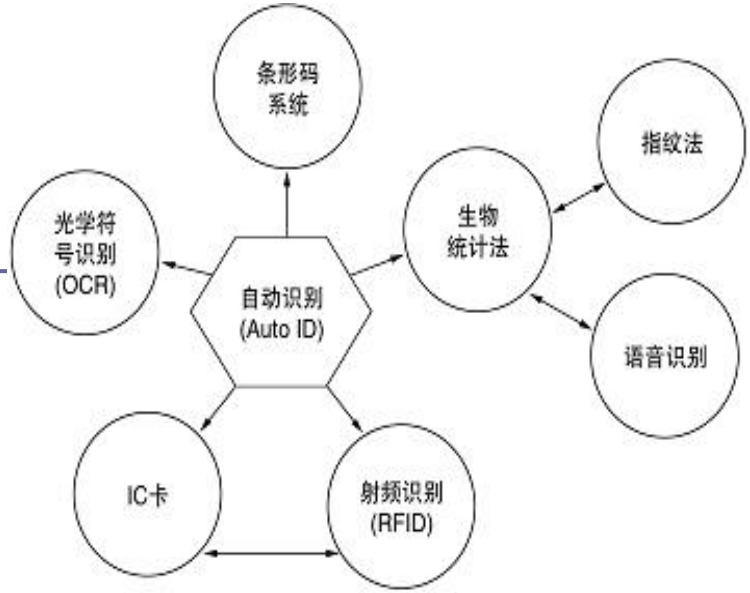
RFID射频识别技术

- 技术概述
- RFID基本原理
- RFID编码体系
- RFID协议标准
- RFID系统应用案例

什么是RFID?

- RFID = radio frequency + identification
- 射频识别，俗称电子标签 （射频+标签）
  - 一种非接触式的**自动识别技术**
  - 通过**射频信号自动识别**目标对象并获取相关数据，无须人工干预
  - 能够存储信息，是信息收集系统的信息载体
  - 能够被附着在物体或包含在物体中
  - 取代已经有几十年历史的条形码技术

自动识别技术比较



- 条形码识别（bar code）
  - 一种特殊的二值代码。代码按照事先规定的图序，以平行排列的线条和分隔的间隙组成了数据。
  - 由宽的和窄的线条或间隙组成的序列可以通过激光扫描读出。
  - 应用：货物管理
  - 二维码：用某种特定的几何图形按一定规律在平面分布的黑白相间的图形记录数据
- 智能卡识别（IC卡）
  - IC卡插入阅读器，阅读器的接触弹簧与IC卡的触点产生电流接触，阅读器通过接触点给IC卡提供能量和定时脉冲，阅读器与IC卡间通过双向串行接口（I/O）进行数据传输。分为存储器卡和微处理器卡。
  - 应用：现金卡、SIM卡
- 射频识别（RFID）
- 光学符号识别（OCR）
  - 文字提取
- 生物识别
  - 指纹识别
  - 语音识别
  - 眼底视网膜识别

自动识别技术（2）

系统参数	条码	光学符号识别	语音识别	生物计数测量法	IC卡	射频识别系统
典型的数据量/字节	1～100	1～100		-		
数据密度	小	小	高	高	很高	很高
机器阅读的可读性	好	好	费时间	费时间	好	好
个人阅读的可读性	受制约	简单容易	简单容易	困难	不可能	不可能
受污染/潮湿影响	很严重	很严重	-	-	可能（接触）	没有影响
受光遮盖影响	全部失效	全部失效	-	可能	-	没有影响
受方向和位置影响	很小	很小	-	-	一个插入方向	没有影响
用坏/磨损	有条件	有条件的	-	-	接触	没有影响
购置费/电子阅读设备	很少	一般	很高	很高	很少	一般
工作费用（例如：打印机）	很少	很少	无	无	一般（接触）	无
未经准许的复制/修改	容易	容易	可能（录音）	不可能	不可能	不可能
阅读速度（包括数据载体的使用）	低-4s	低-3s	很低>5s	很低>>5～10s	低～4s	很快
数据载体与阅读器之间的最大距离	0～50cm	<1cm（扫描器）	0～50cm	直接接触	直接接触	0～5m微波

RFID技术发展历史

- RFID直接继承了雷达的概念，并由此发展出一种生机勃勃的“自动识别”新技术——RFID技术。
- 二次世界大战期间，英军使用类RFID技术来识别友军或敌军的飞机。
- 1948年哈里.斯托克曼发表的“利用反射功率的通讯”奠定了射频识别RFID的理论基础。
- 1951—1980年。RFID技术理论发展，开始应用尝试。出现了一些最早的RFID应用。
- 1981～1990年。商业应用阶段，各种规模应用开始出现。
- 1991～2000年。开始RFID技术标准化研究，RFID产品得到广泛采用，RFID产品逐渐成为人们生活中的一部分。
- 2001—今。标准化问题日趋为人们所重视，RFID产品种类更加丰富，有源电子标签、无源电子标签及半无源电子标签均得到发展，电子标签成本不断降低，规模应用行业扩大。

RFID 的应用

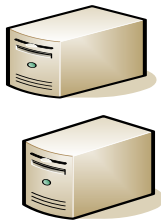
- 物流领域：食品安全追溯、库存管理、运输管理、物料清点、废弃物管控、 航空运输的行李识别
- 电子票务　景点门票、演出门票、门禁及上下班人事管理
- 医疗应用：　医院的病历系统、危险或管制之生化物品管理
- 交通运输：　高速公路的收费系统、车辆识别等
- 防盗应用：　超市的防盗、图书馆或书店的防盗管理
- 动物监控：　畜牧动物管理、宠物识别、野生动物生态追踪
- 自动控制：　汽车、家电、电子业之组装生产
- 联合票证：　联合多种用途的智能型储值卡、积分卡
- 防伪应用：酒类、化妆品、名表等

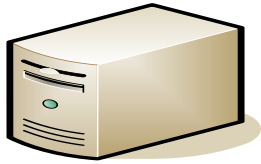
RFID 基本原理

- RFID系统组成
- RFID系统工作原理
- RFID标签
- RFID读写器
- 天线
- 防碰撞

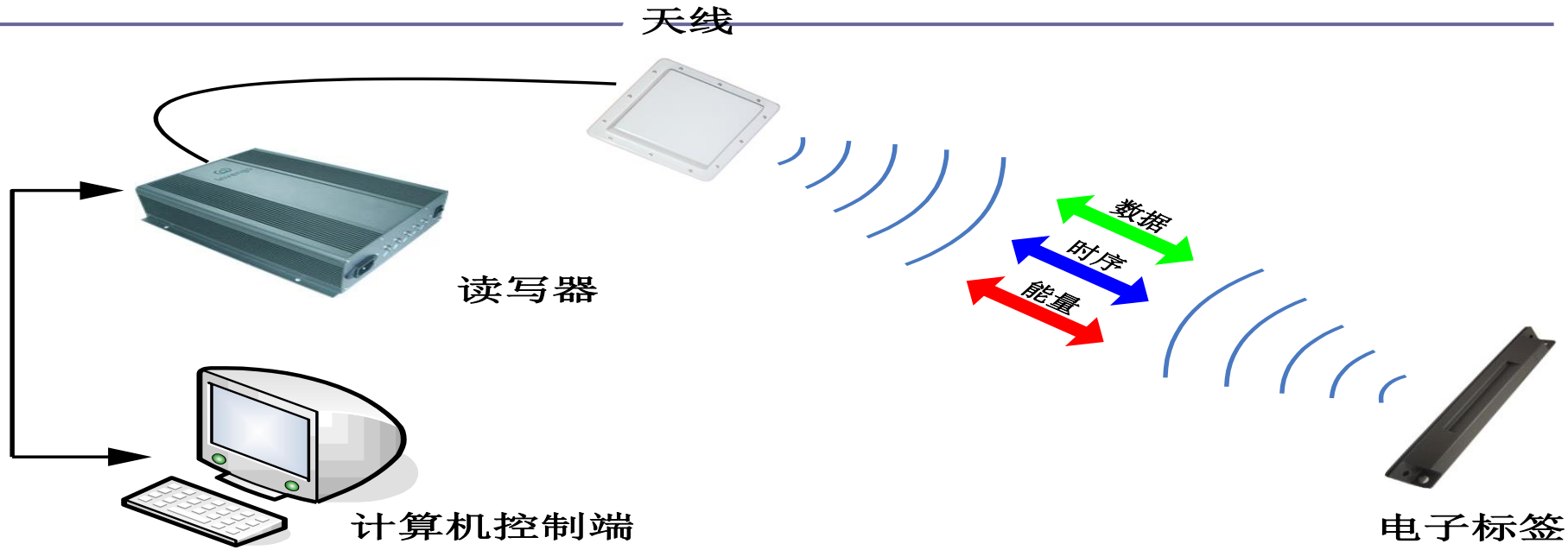
RFID系统组成

- **电子标签**由天线和专用芯片组成。
- **阅读器（读写器）**通过天线与RFID电子标签进行无线通信，可以实现对标签识别码和内存数据的读出或写入操作。
- **天线**在标签和读取器间传递射频信号。
- **计算机系统**完成各种基于RFID的应用





RFID系统组成



读写器向电子标签发送射频信号，电子标签进入射频信号的识别区域后，将产生感应电流从而获得能量，并将电子标签信息通过天线发送出去。

读写器将电子标签信息利用解码器进行解码，再通过网络或RS232等接口将标签信息传送到计算机进行处理

RFID标签

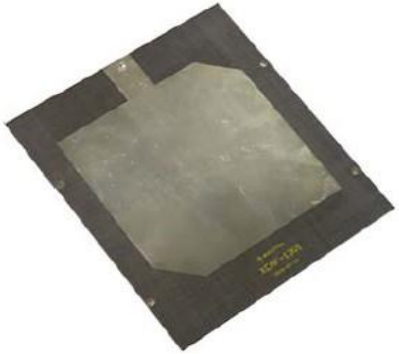
查看群文件:　第三章示例-标签.mp4

标签分类

- 按读写方式分
  - 只读　　写入一次读取多次　　重复读写
- 按记忆容量分
  - 只读：大多仅具备Tag ID，无多余记忆容量
  - 其它：64bits-256 bits为主流，但也有高达数K容量产品。
- 按供电方式分
  - 被动：reader供电
  - 主动：自带电池，提供信号发射能量
  - 半被动：自带电池，提供CPU工作能量

RFID--读写器

RFID—天线



UHF标签举例

ALL-9238 tag
"SquiggleT" antenna design;
Approximate Size: 95mm x 10mm; Small UHF form factor

ALL-9250 tag
”I2” antenna design;
Approximate Size: 134mm x 13mm; high gain in a controlled orientation

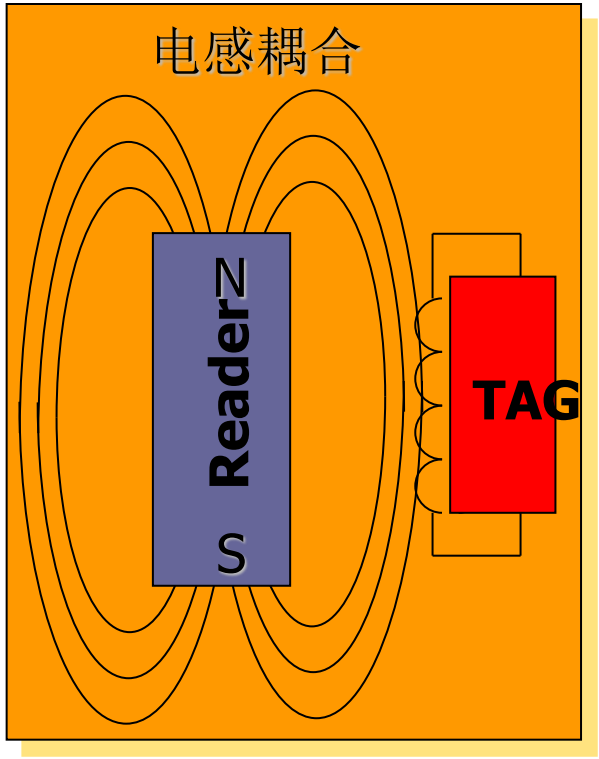
ALL-9254 tag
"M" antenna design
Approximate Size: 95mm x 30mm
Very high gain

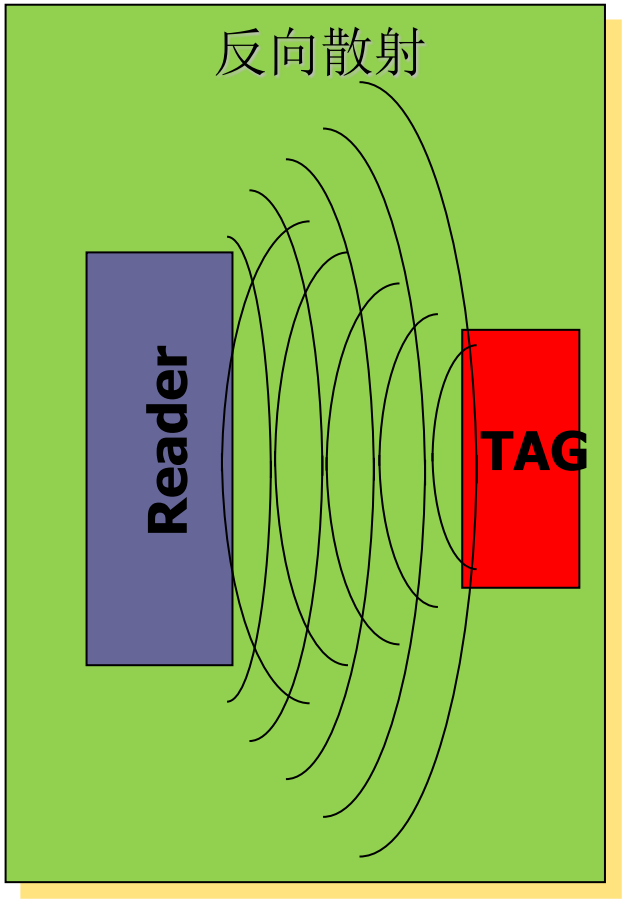
RFID的工作频率

- 按工作频率的不同分为：
  - 低频（LF）(125KHz--135KHz)
  - 高频（HF）(13.56MHz)
  - 超高频（UHF）（860MHz--960MHz ）
  - 微波（MW）2.45GHz、5.8GHz

标签与读写器间的耦合类型（1）

- 电感耦合
- 反向散射耦合





标签与读写器间的耦合类型（2）

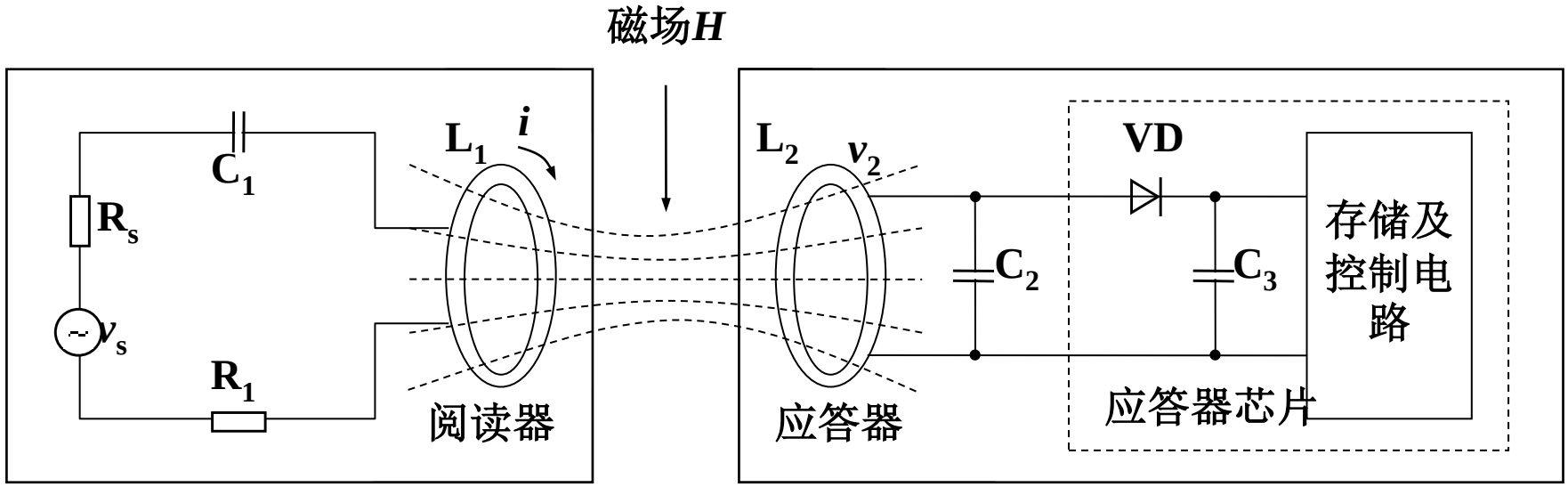
- 电感耦合
  - 利用电感（磁）耦合构成射频通道，
  - 典型作用距离：10cm左右
  - 工作频率：125K、6.75M、13.56MHz
  - 负载调制方式传输数据
  - 低成本RFID系统的主流

标签与读写器间的耦合类型（3）

反向散射耦合

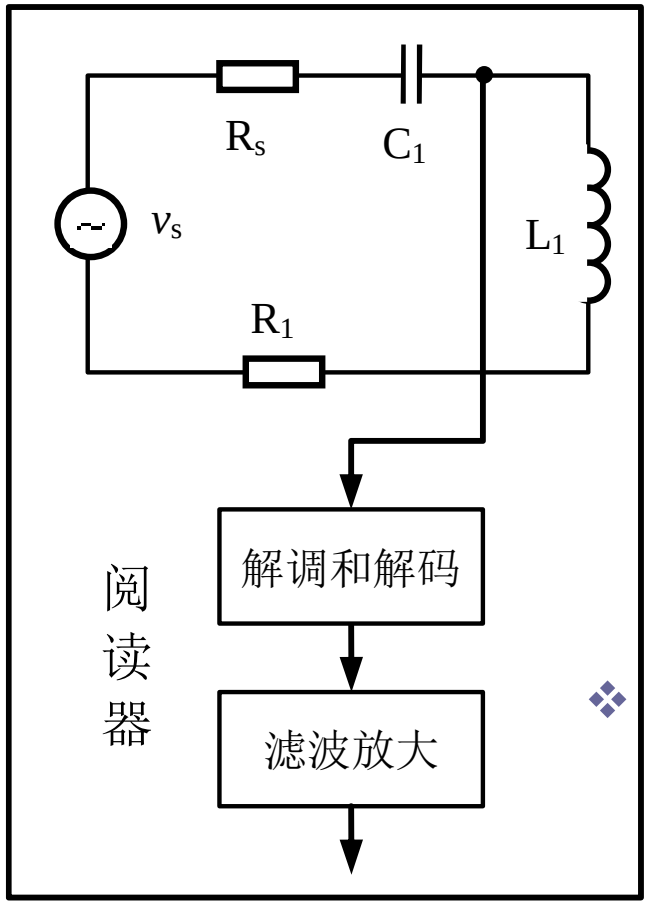
- 利用辐射远场区的电磁耦合（电磁波的发射与反射）构成射频通道，
- 典型作用距离 1-10m
- 工作频率：433M、915M、2.4G、5.8GHz
- 反射调制方式传输数据
- 高速移动物体远距离识别
- 目前发展最快的RFID系统

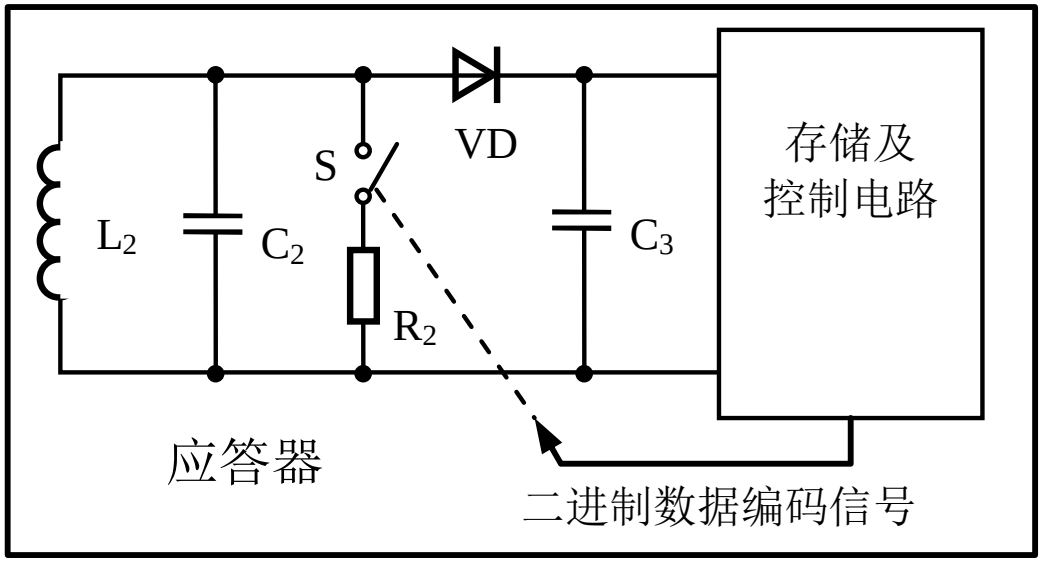
电感耦合（磁耦合）（1）



- **Tag的能量供给**
  - 工作距离：10cm以下；工作频率：13.56MHz，<135KHz
  - 无源标签：电感线圈 L1和 L2看做变压器的初次级线圈，通过交变磁场H的感应，在L2上产生电压，供tag使用
  - 电感耦合效率较低，适于小电流电路

电感耦合（磁耦合）（2）

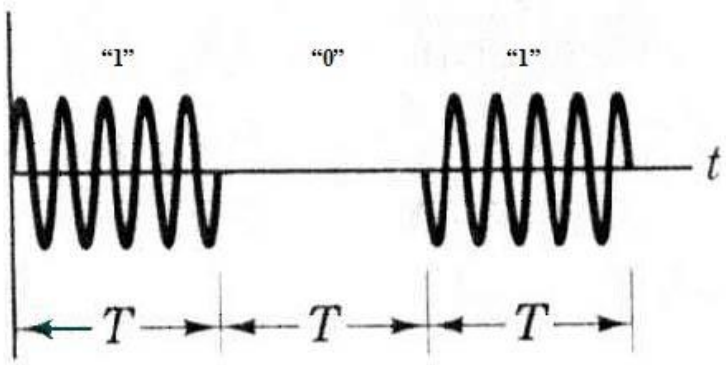


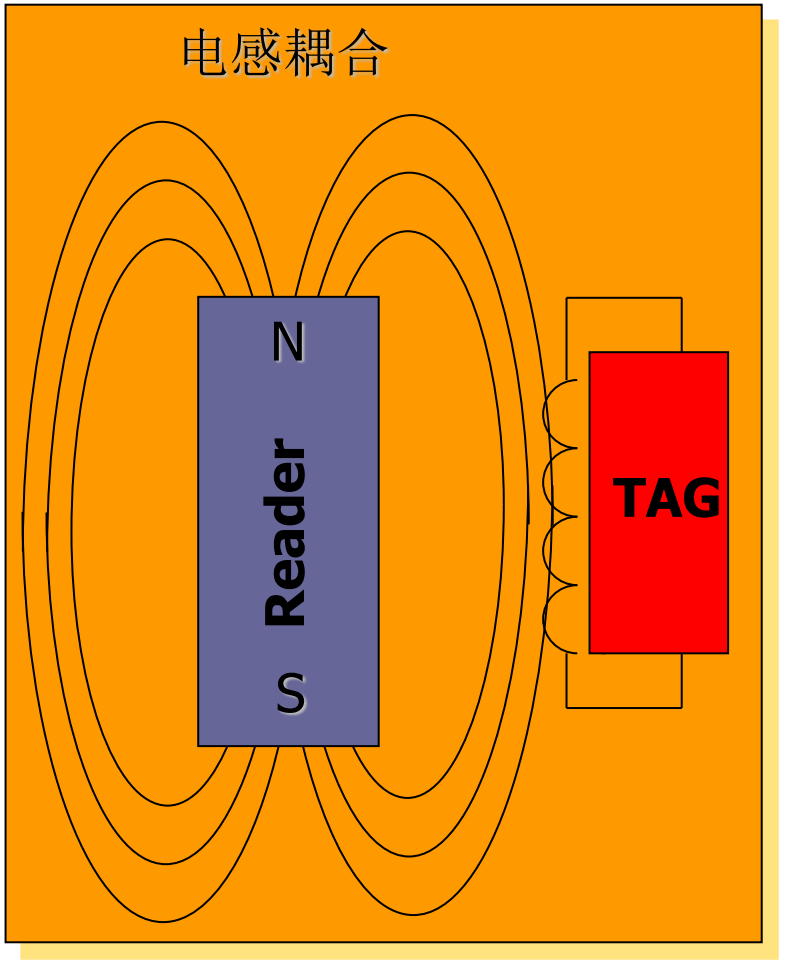


- **Tag→reader：负载调制**
  - **Tag上二进制编码值控制S的通断**
  - **L2上电流的变化引起L1上电压的变化**
  - **Reader识别该电压变化，产生信息**
  - **属于振幅调制**

电感耦合（磁耦合）（3）

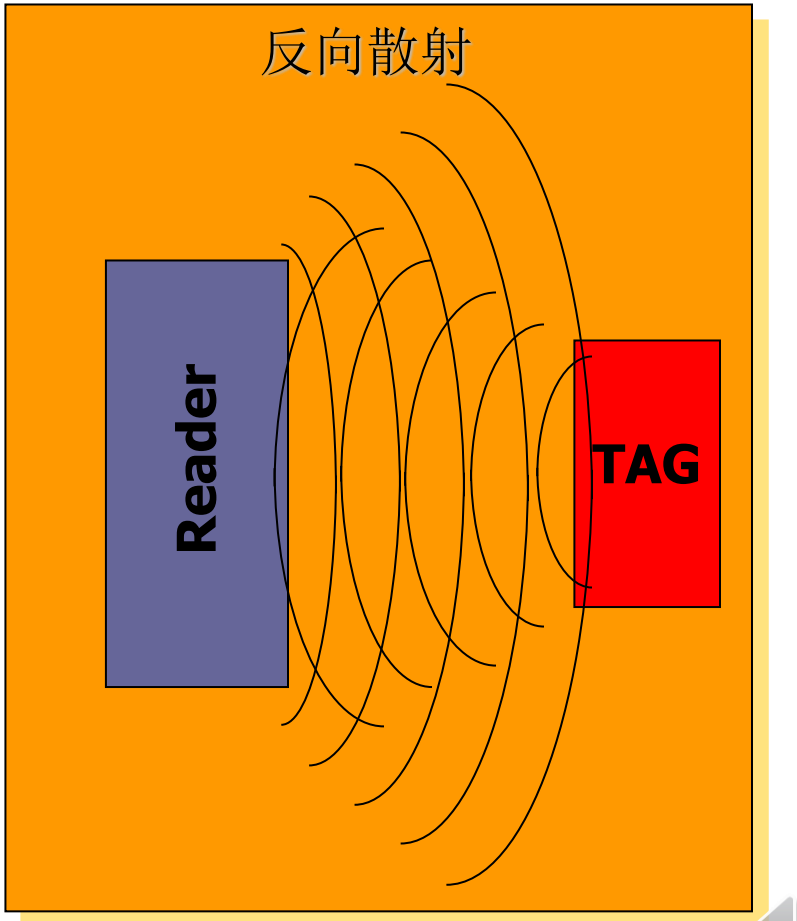
- **reader → Tag 数据传输**
  - **ASK数字调制方式**





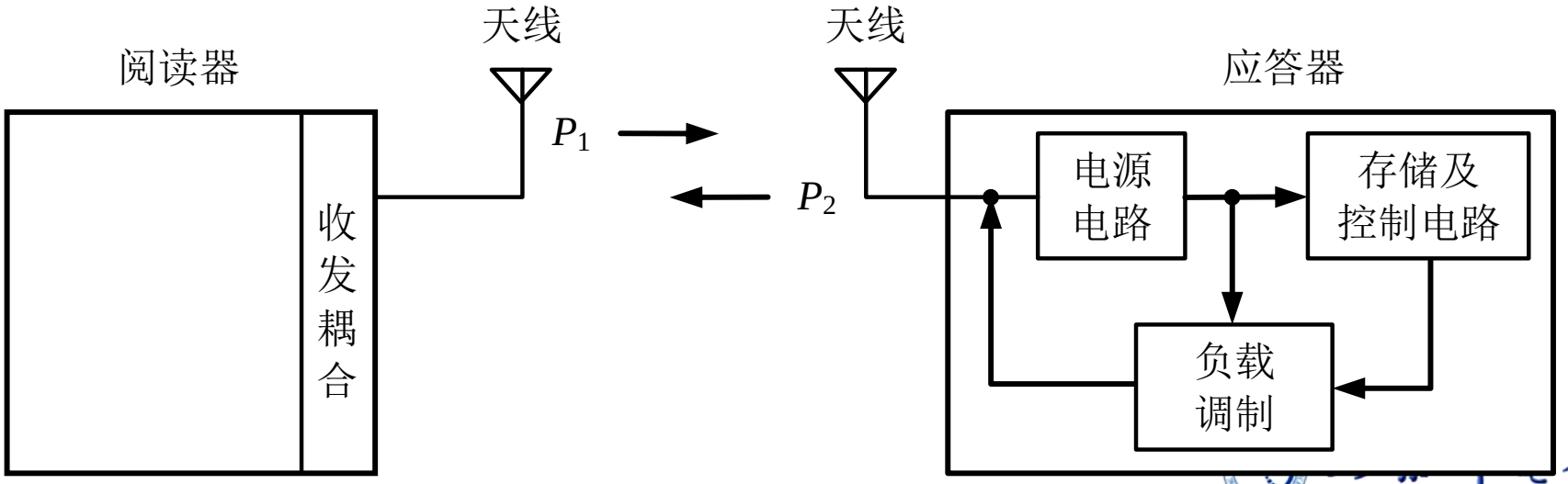
反向散射耦合方式（1）

- 反向散射
  - 源于雷达技术
  - 电磁波遇到空间目标时，能量的一部分被物体吸收，另一部分以不同强度被散射到各个方向
  - 散射的能量中，一部分反射到发射天线，并被接收和识别，即可获得目标的有关信息



反向散射耦合方式（2）

- 工作频率：UHF和MW；
- 工作距离：>1m
- Tag的能量供给：Reader发射的功率P1衰减后到达tag，tag吸收该功率P1’，整流后供电
- Tag→Reader：反光镜原理，tag通过“天线开关”控制天线的阻抗，改变天线的反射系数，实现类似ASK的数字调制



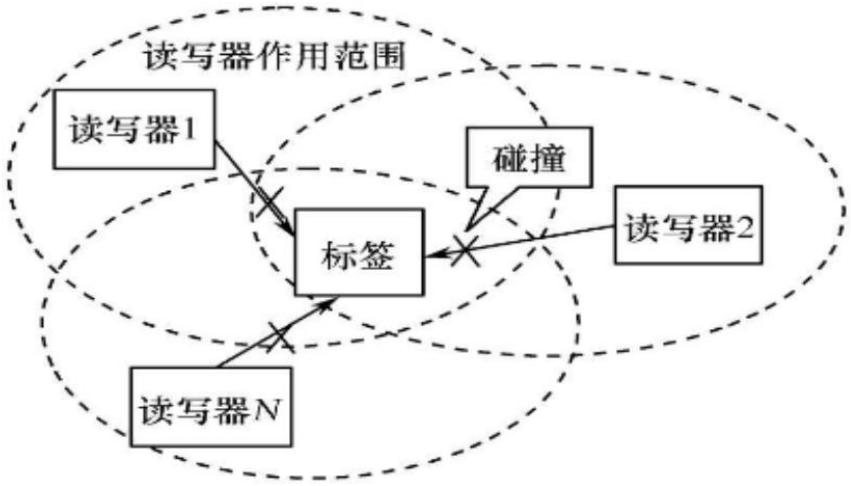
RFID系统的碰撞

- 在RFID系统中多个读写器以及多个标签同时出现的应用场合，会导致读写器之间或标签之间的互相干扰，这种冲突干扰就是碰撞
  - 1）多标签碰撞，多个标签与同一个读写器同时通信时产生的碰撞。
  - 2）多读写器碰撞，多个读写器在信号交叠区域内产生干扰，导致读写器的阅读范围降低，严重时甚至无法读取标签。

防碰撞

多读写器碰撞

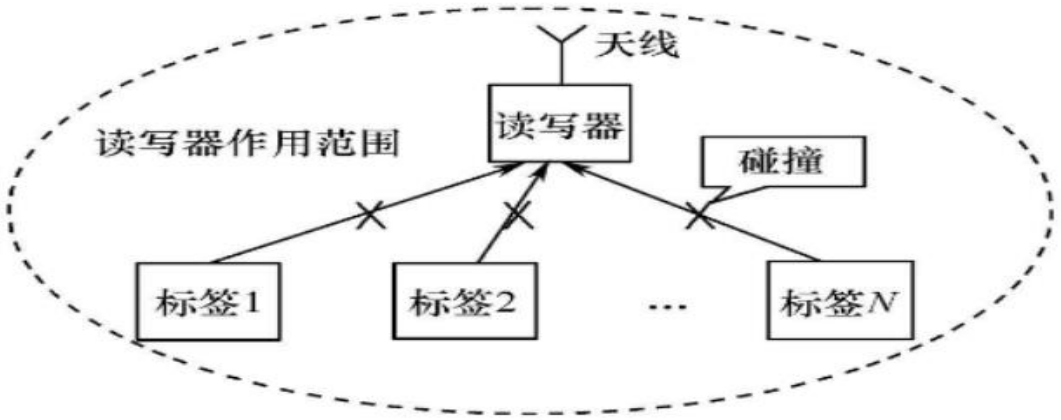
- 当相邻的读写器作用范围有重叠时，多个读写器同时读取同一个标签时可能会导致多个读写器与标签之间的干扰。
- 图中标签同时收到3个读写器的信号，标签无法正确解析读写器发来的查询信号。
- 读写器本身有能量供应，能进行较高复杂度的计算，可以检测到碰撞的发生。
- 读写器之间可以互通来解决读写器的碰撞问题，比如读写器调度算法和功率控制算法。



防碰撞

多标签碰撞

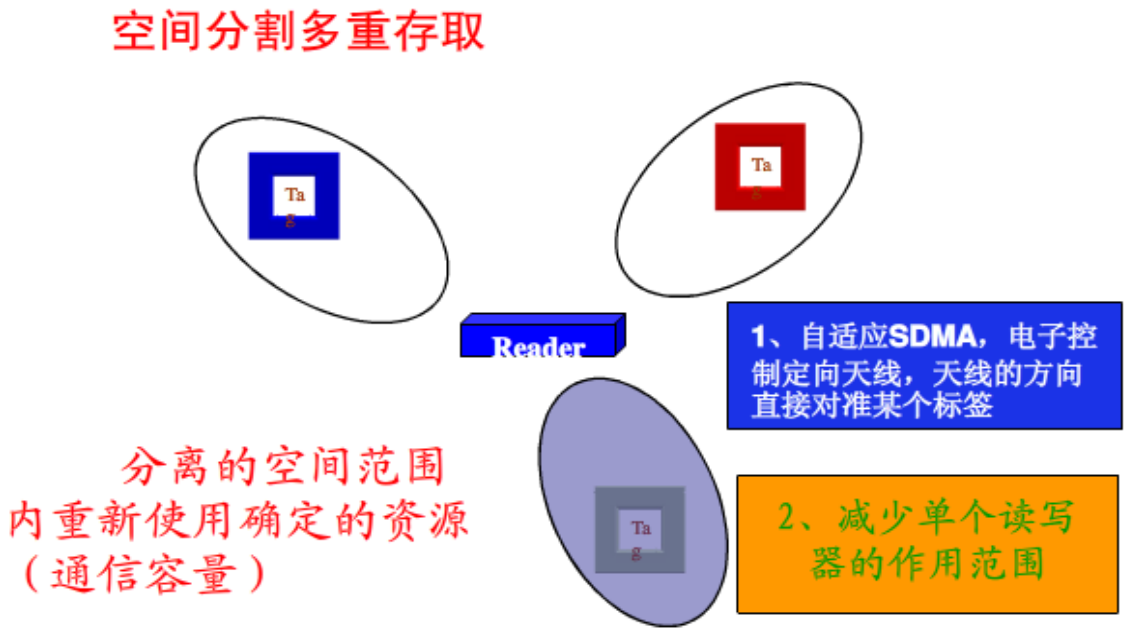
- 多标签碰撞是读写器同时收到多个标签信号，导致无法正确读取标签信息的问题。
- 读写器发出识别命令，标签在应答中会出现多个标签同时时刻应答，或一个标签还未完成应答是其他标签就发出应答。
- 标签之间的信号互相干扰，导致标签无法被正常读取。



多标签防碰撞

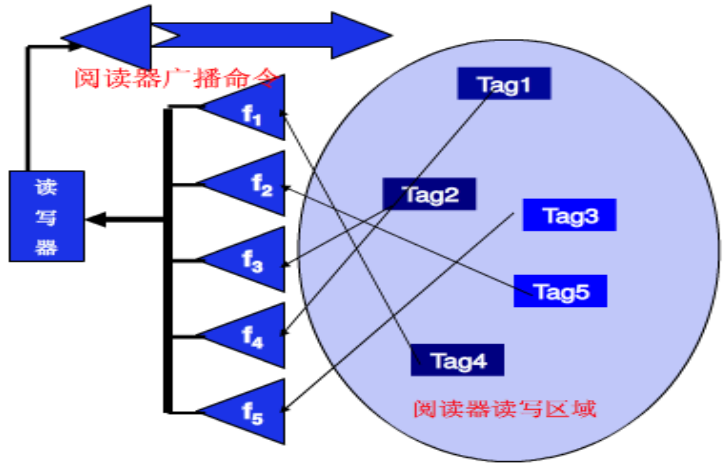
无线通信中的防碰撞方法，解决防碰撞的方法主要包括**空分多路SDMA、频分多路FDMA 、码分多路 CDMA 、时分多路 TDMA**

- 空分多路法是在分离的空间范围内实现多个目标识别。
  - 一种实现方法是将读写器和天线之间的作用距离按照空间区域进行划分
  - 一种实现方法是读写器利用相控阵天线
  - 空分多路法的缺点是天线系统复杂，会大幅度提高成本。



多标签防碰撞

- 频分多路FDMA是将若干个使用不同载波频率的调制信号，在同时供通信用户使用的信道上进行传输的技术。
- 通常，RFID系统中读写器到标签的前向链路工作频率是固定的，可以用于能量的供应和数据的传输。
- 对于反向链路，不同标签采用不同频率的载波进行数据调制，信号间不会产生干扰，读写器对接收到的不同频率信号进行分离，
- 从而实现对不同标签的识别。
- 频分多路法的缺点是读写器和标签成本较高

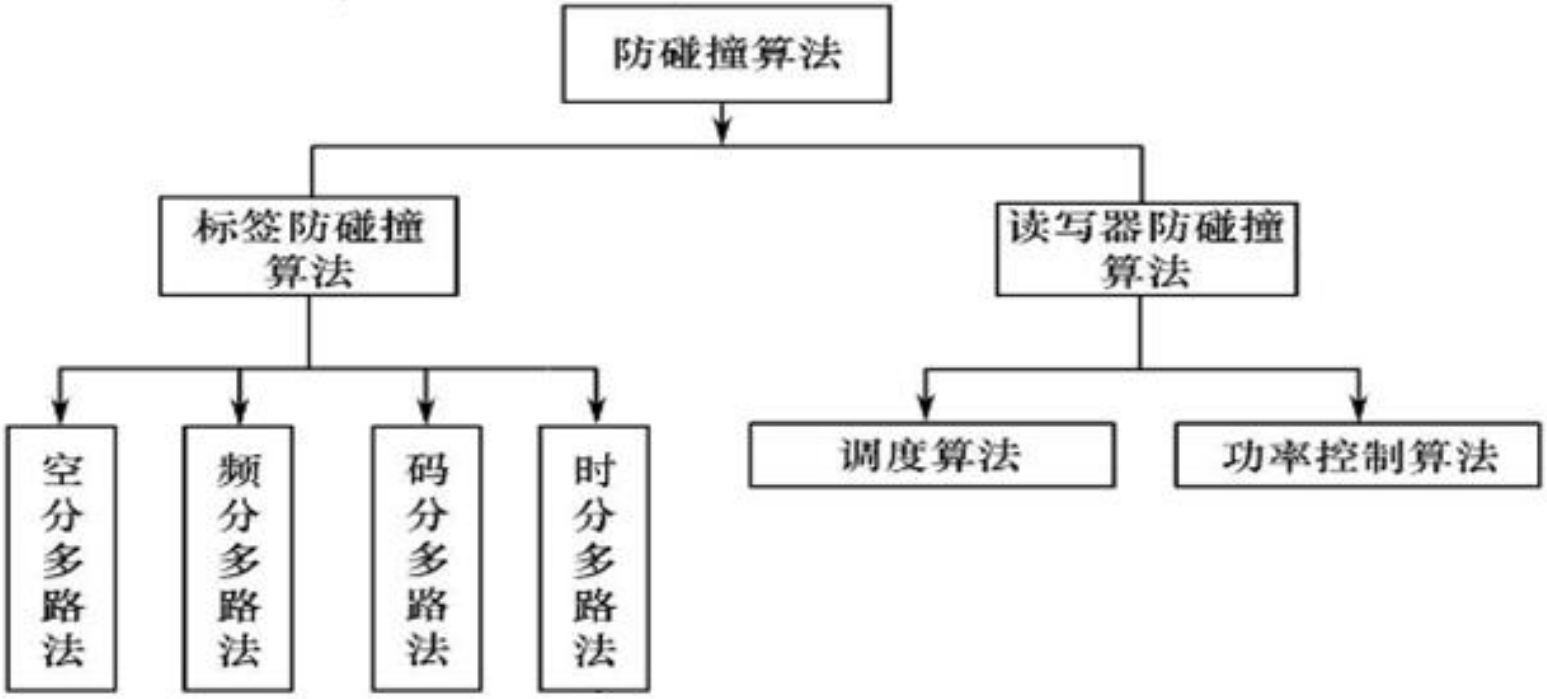


多标签防碰撞

- 码分多路CDMA 是基于扩频通信技术发展来的。扩频技术包括扩频与多址两个基本概念。多址就是给每个用户分配一个地址码，每个地址码相互正交。
- 码分多路抗干扰性好，保密安全性高。但该方法在接收时地址码捕获时间长、伪随机码的产生选择较难。

- 时分多路TDMA是把整个可供使用的通路容量按照时间分配给多个用户的技术。
- 时分多路复用是按照传输信号的时间进行分割的。

防碰撞算法分类



RFID 编码体系

- EPC global标准体系与EPC编码
  - 1999年美国麻省理工学院成立Auto-ID中心，进行RFID技术研发，通过创建RFID标准，并利用网络技术，形成EPC系统
  - 为实现和管理EPC的工作，国际物品编码协会在2003年11月成立了全球电子产品代码中心EPC global
  - EPC统一对全球物品的编码方法，直到编码至单个物品
  - EPC规定了将此编码以数字信息的形式存储于附着在物品上的标签中
  - 阅读器通过无线空中接口读取标签中的EPC码，并经计算机网络传送至信息控制中心，进行相应的数据处理

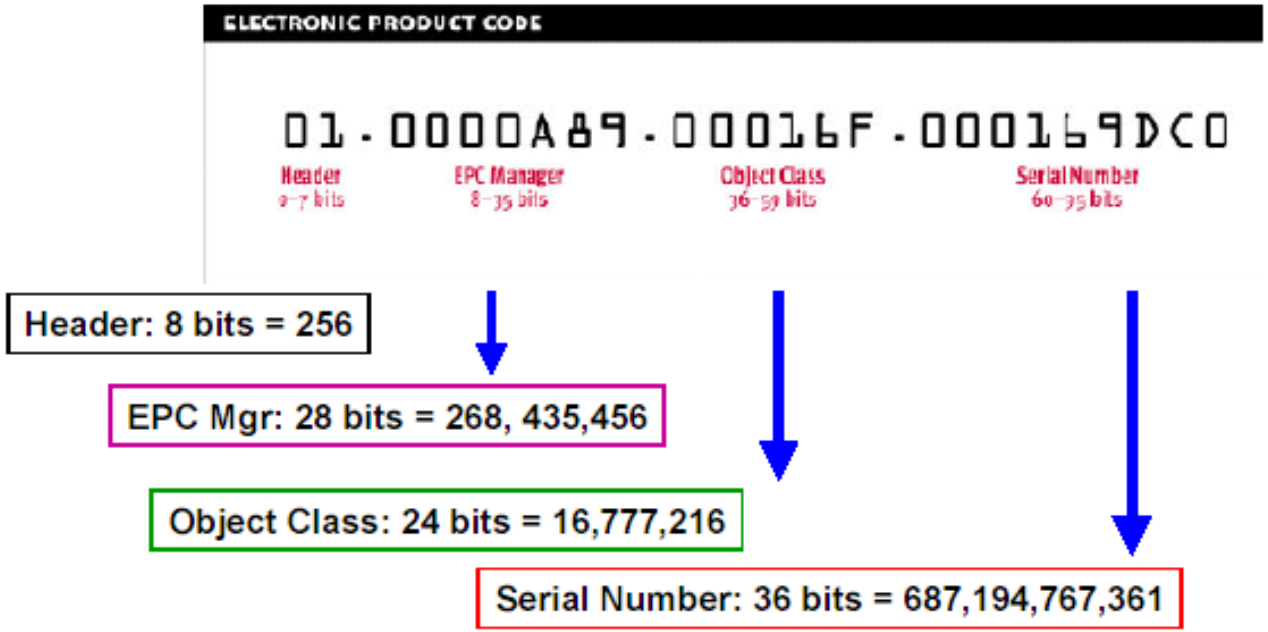
EPC编码规则

EPC编码结构中各字段的长度（位）

编码类型		版本号	域名管理	对象分类	序列号
EPC64	TYPE I	2	21	17	24
	TYPE II	2	15	13	34
	TYPE III	2	26	13	23
EPC96	TYPE I	8	28	24	36
EPC-256	TYPE I	8	32	56	160
	TYPE II	8	64	56	128
	TYPE III	8	128	56	64

- 版本号字段标识EPC的版本号；
- 域名管理字段标识相关的生产厂商信息；
- 对象分类字段编码物品精确类型；
- 序列号用于编码出唯一物品。

EPC Data Standard- 96 bit



Header - Tag version number
EPC Manager - Manufacturer ID
Object class - Manufacturer's product ID
Serial Number - Unit ID

With 96 bit code, 268 million companies can each categorize 16 million different products where each product category contains up to 687 billion individual units

RFID协议标准

- RFID的ISO/IEC标准
- UHF 协议过程
  - 标签存储区格式
  - 协议命令

低频LF RFID标准及应用

相关标准	ISO11784/11785 ISO/IEC18000-2
工作频率	频率范围为30kHz - 300kHz。典型工作频率有：125KHz，133KHz。
工作方式	电感耦合，标签需位于阅读器天线辐射的近场区内
阅读距离	一般情况下小于0.1米
数据传输	低速、数据少
应用方向	低端应用，动物识别

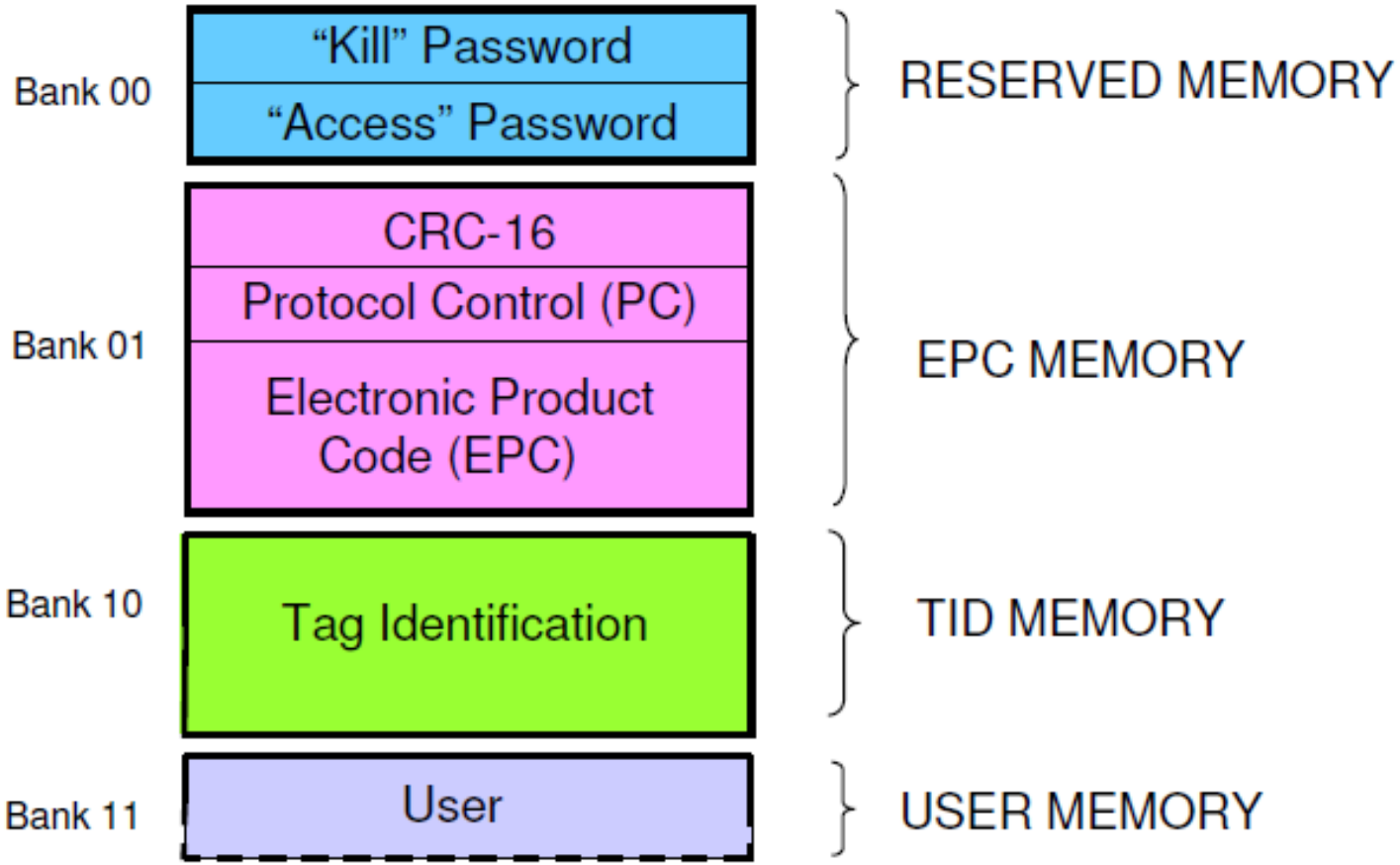
高频HF RFID标准及应用

相关标准	ISO/IEC14443, ISO/IEC18000-3
工作频率	频率范围为3MHz -30MHz。典型工作频率有：13.56MHz
工作方式	电感耦合，标签需位于阅读器天线辐射的近场区内
阅读距离	一般情况下小于1米
数据传输	中速数据传输
应用方向	门禁、身份证、电子车票、电子闭锁

超高频UHF RFID标准及应用

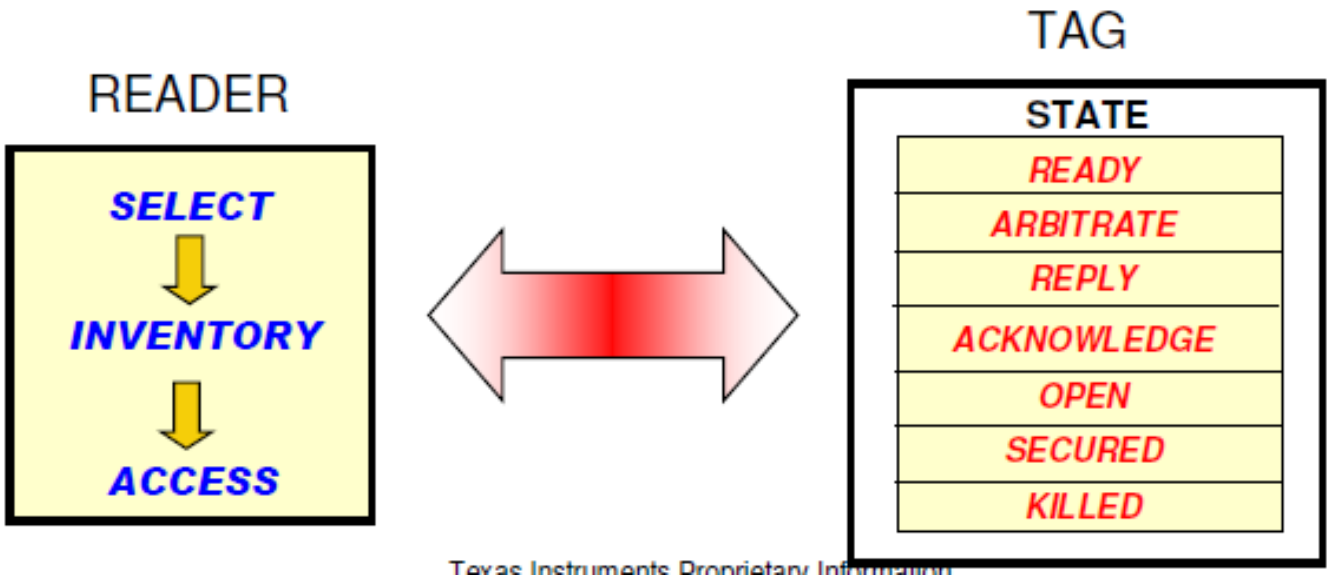
相关标准	ISO/IEC18000-4、-5、-6、-7
工作频率	433MHz，862(902)-960MHz，2.45GHz，5.8GHz
工作方式	电磁耦合，标签位于阅读器天线辐射的远场区内
阅读距离	阅读距离一般大于1m，典型情况为4-6m，最大可达10m以上
数据传输	可以承载更高的数据传输速率，更适合快速、大容量高效的物品识别
应用方向	移动车辆识别、电子身份证、仓储物流应用、海量物品快速识别

UHF 标签存储区格式

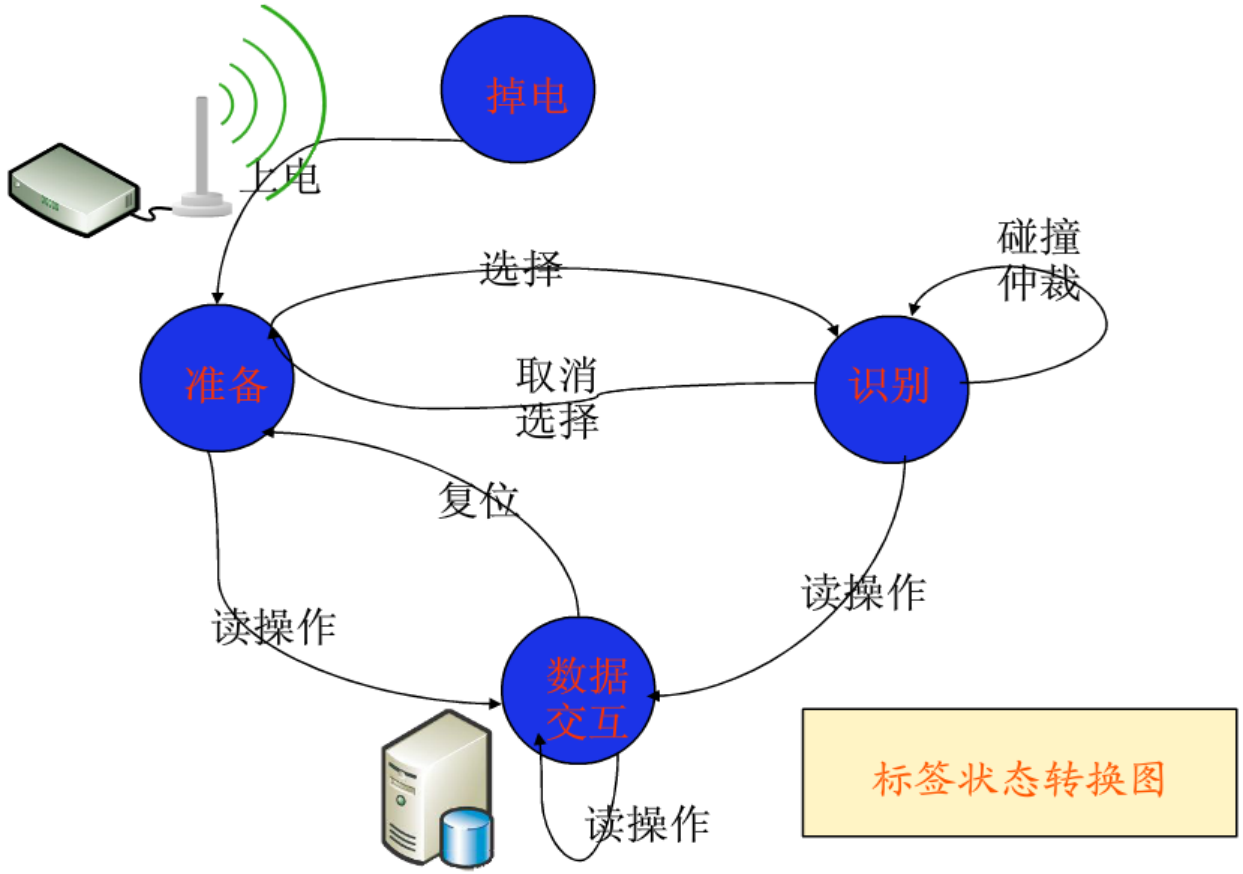


UHF 命令

- Three basic operations manage Tag populations
  - *Select* is used to determine which groups of Tags will respond.
  - *Inventory* is used to identify (singulate) individual Tags from a group
  - *Access* is used once Tags have been singulated and individual commands can now be addressed to them

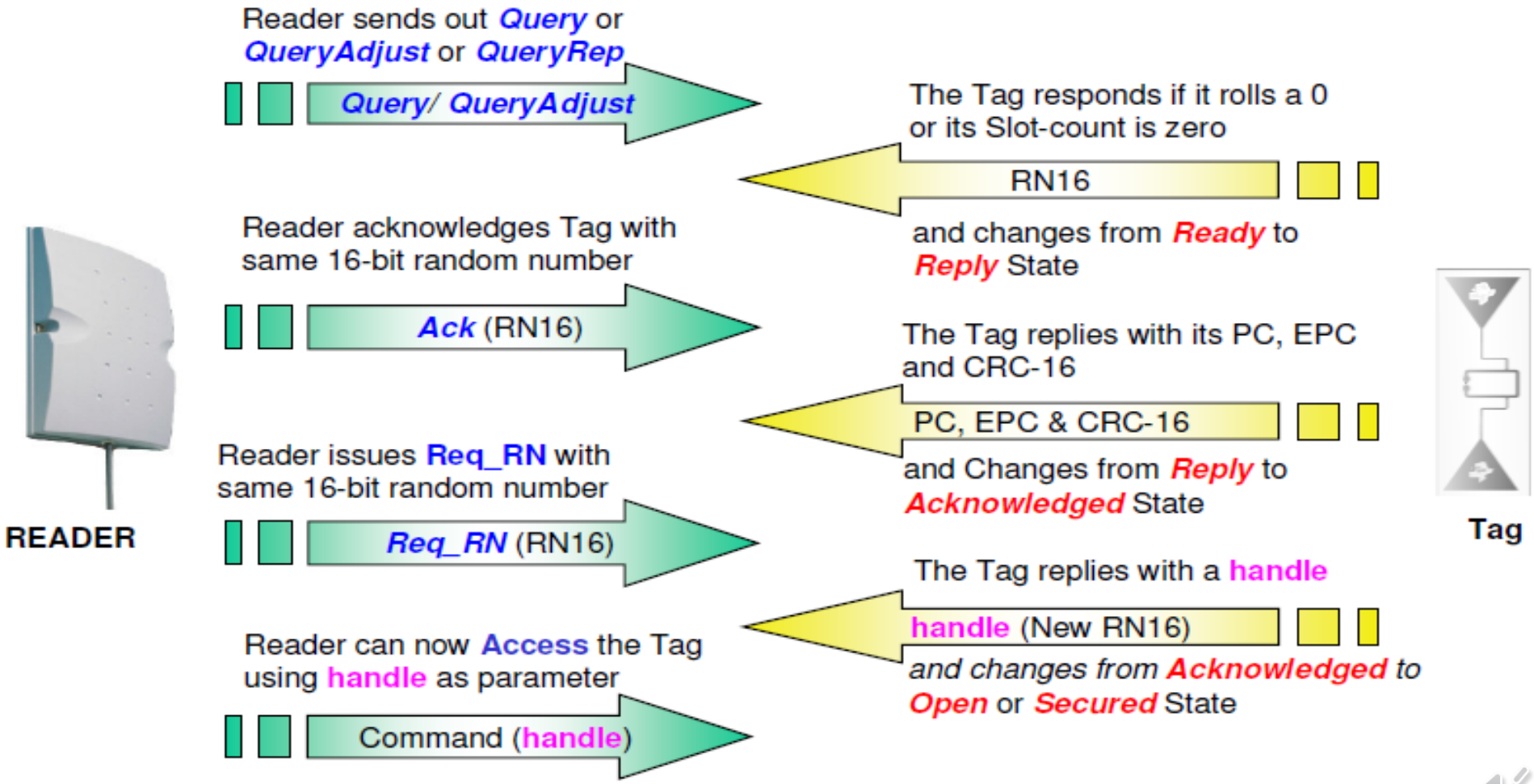


标签状态



标签状态转换图

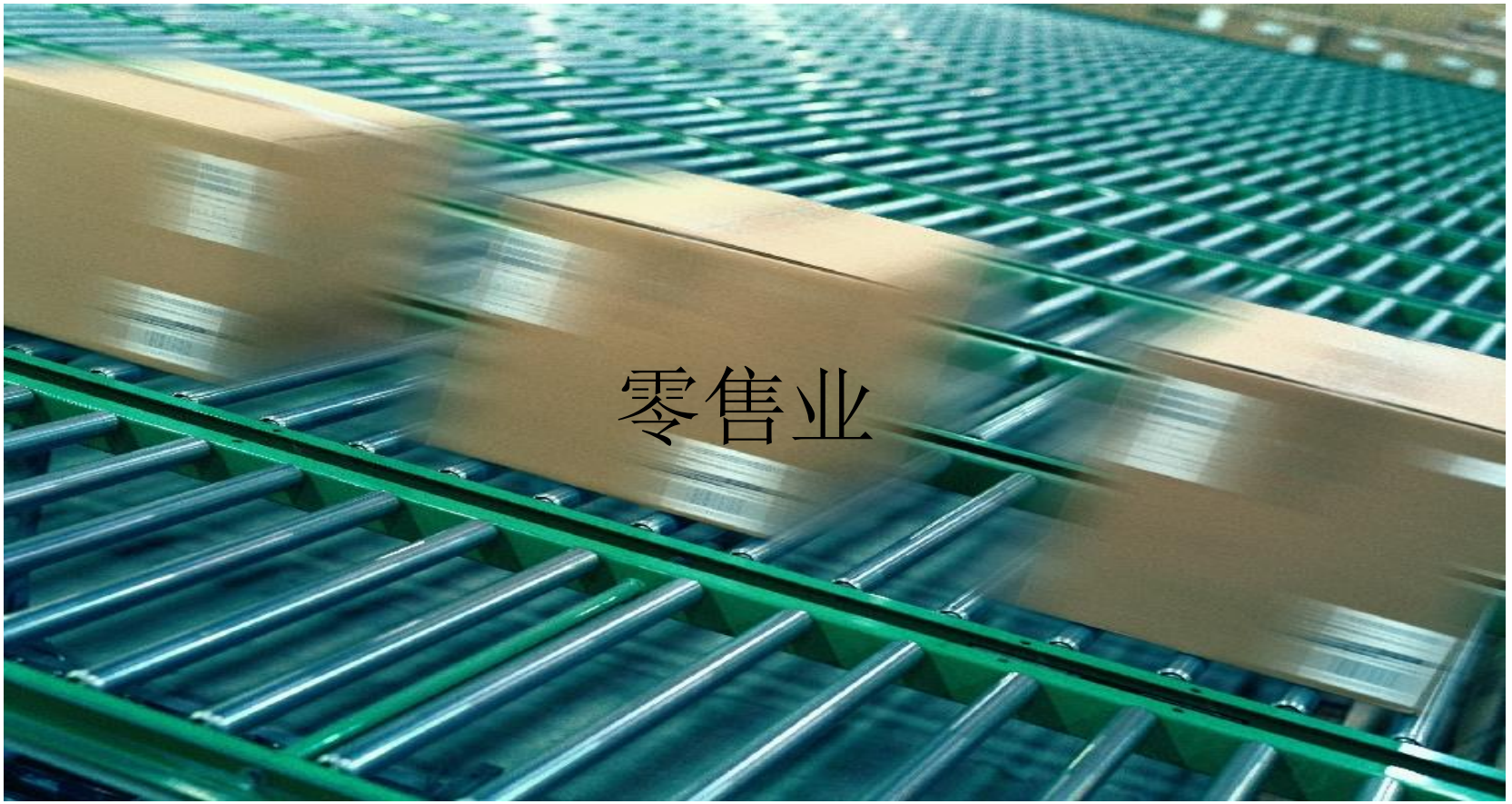
举例：Inventory 命令集



RFID应用系统案例分析

- 零售业
- 制造业和工业
- 航空业
- 制药业
- 交通与车辆管理
- 物流
- 定位

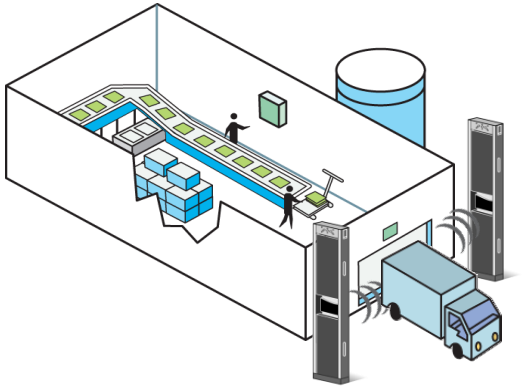
应用与案例研究

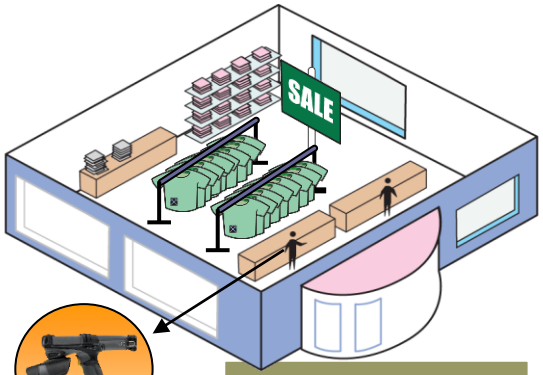


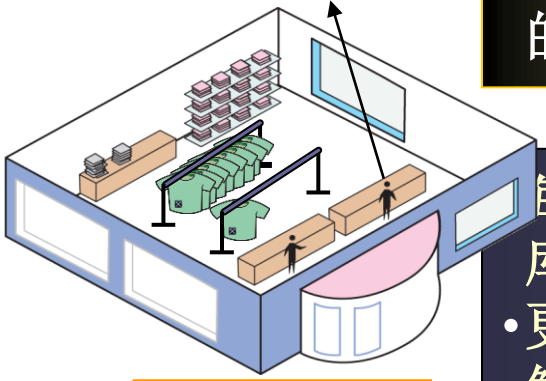
RFID 现状：零售店内可视性

零售商制造工厂

RFID 标签
每个物品







商店 A

商店 B

问题

- 货架和仓库可视性
- 快速补货
- 损失和失窃防范

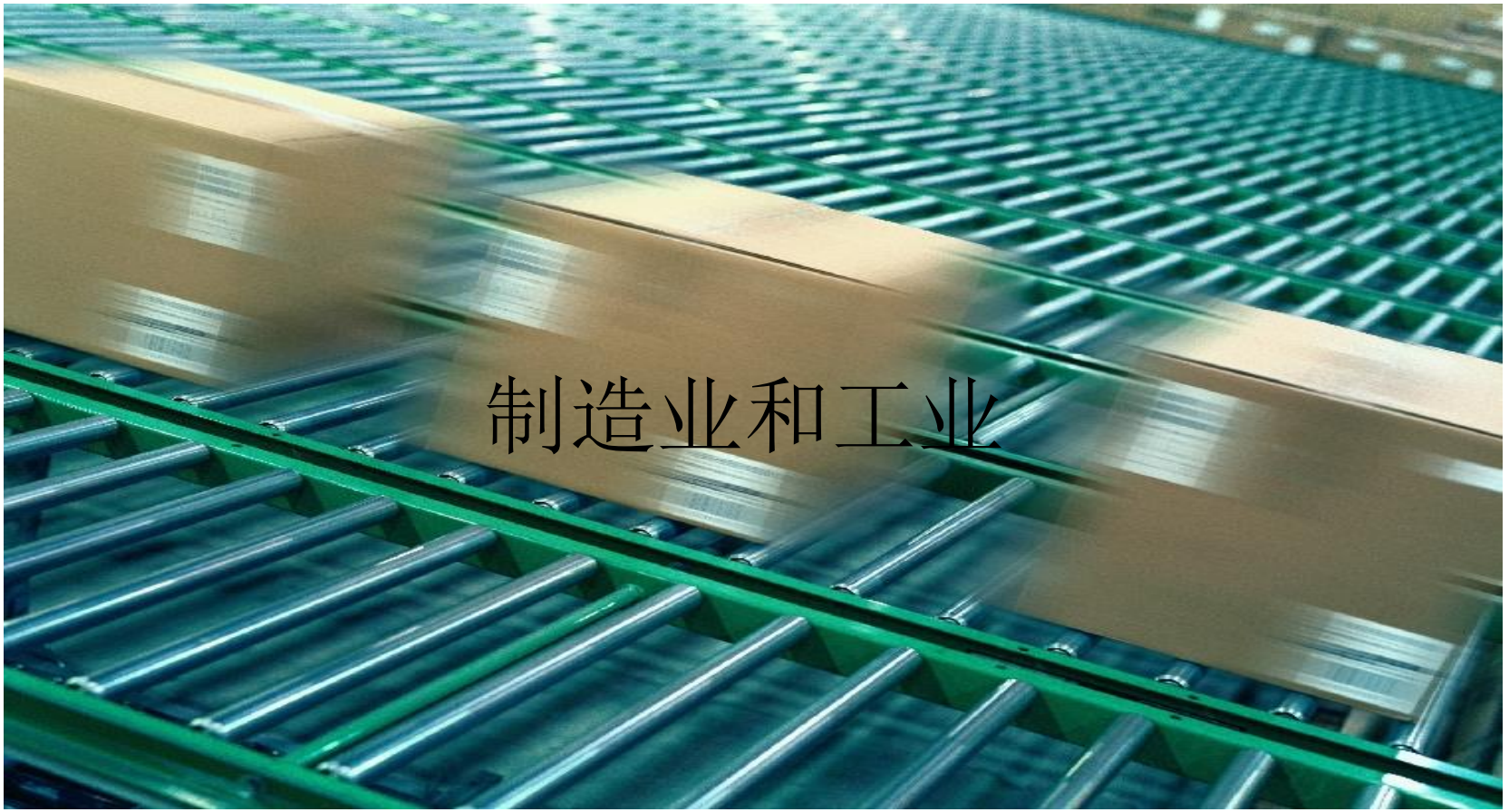
解决方案

- 货物层次上的标签
- 供员工使用的手持式读取器
- 适用于自动库存和物品跟踪的区域读取器

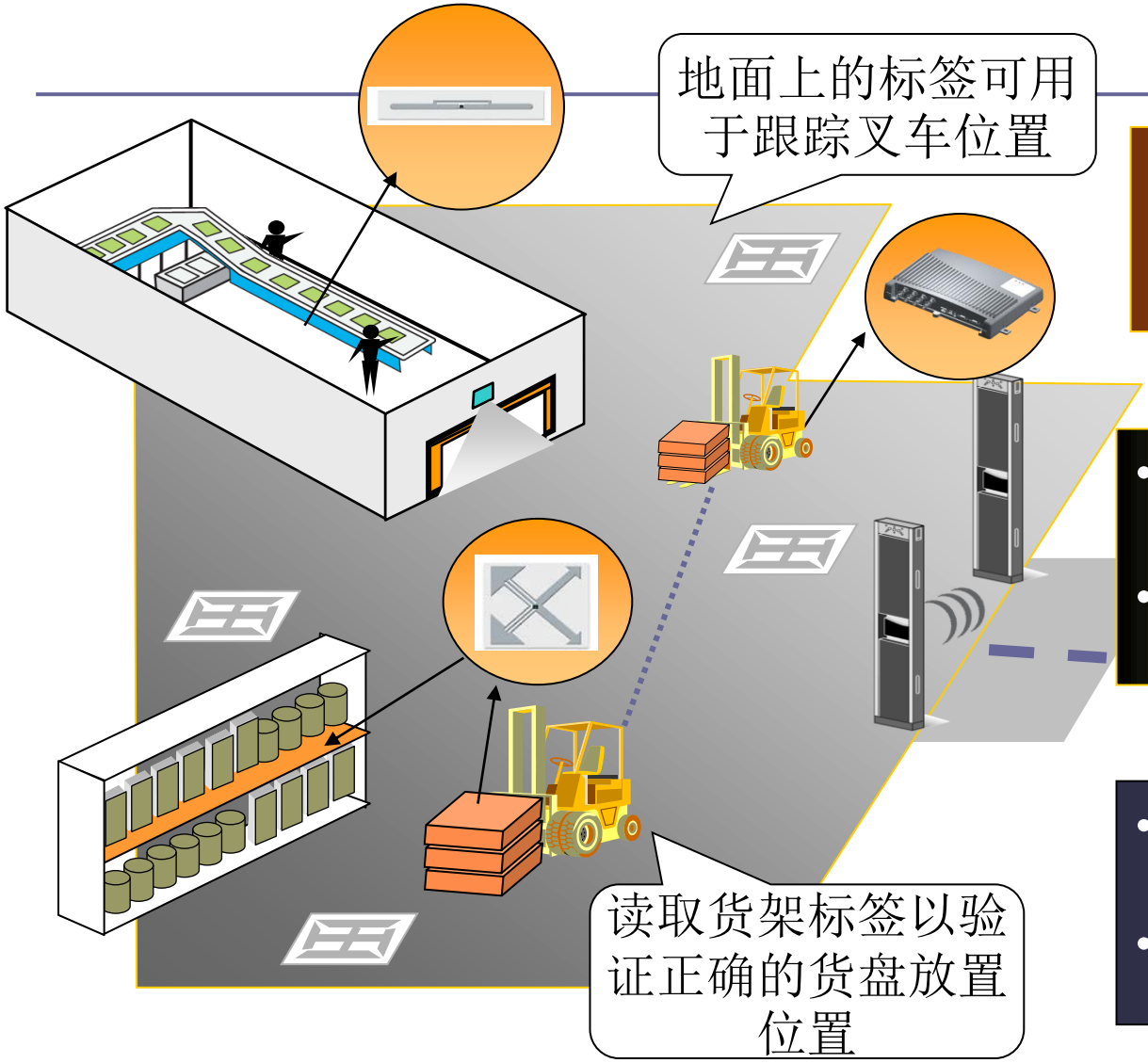
结果

- 每日库存可见性和每周、每月库存可见性
- 更好的货架商品可售性
- 解决产品缺货问题

应用与案例研究



RFID 现状：工业仓库库存跟踪



问题

- 劳动/时间密集型库存流程
- 导致沉淀成本和过期产品损失的错误

解决方案

- 货站入口、传送带和叉车处的 RFID
- 借助地面上的 RFID 标签实现位置可视性

结果

- 装运、收货和检验处理时间缩短了 2 倍至 60 倍
- 配送中心可节省 20% 的运营成本

例子：智能手机与一卡通的交互

查看群文件：RFID 演示.mp4

这个例子中，手机的角色是RFID的reader，公交一卡通是RFID的标签。

Reader与标签进行通信，可以查看到存放在标签里乘车记录与充值记录。

本章内容

- 移动互联网络的各种终端
- 自动识别技术
  - NFC
  - RFID
  - **二维码**

二维码分类

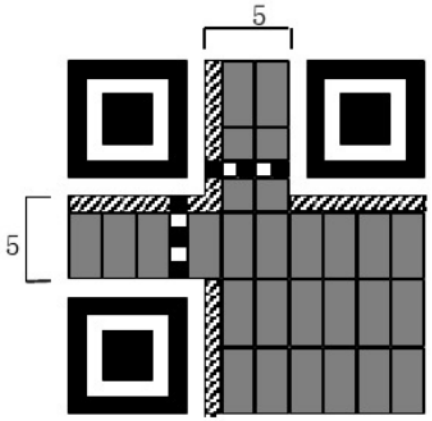
二维码就是通过两个维度（水平方向和垂直方向）来进行数据的编码，通常二维码可以分为两类

1、堆叠式二维码：在一维条形码的基础上，将多个条形码堆积在一起进行编码，常见的编码标准有PDF417等。

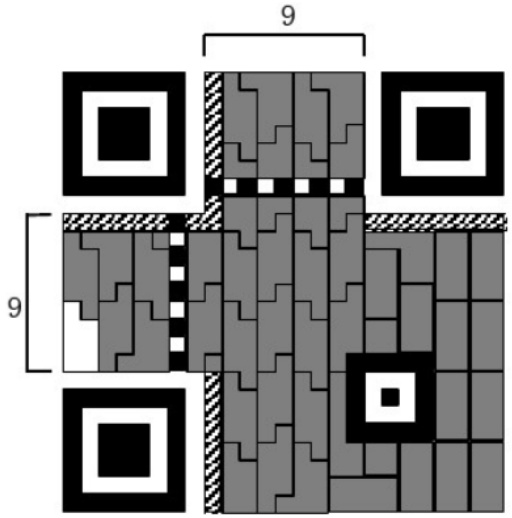
2、矩阵式二维码：在一个矩阵空间中通过黑色和白色的方块进行信息的表示，黑色的方块表示1，白色的方块表示0，相应的组合表示了一系列的信息，常见的编码标准有QR code、 Data matrix。

二维码版本

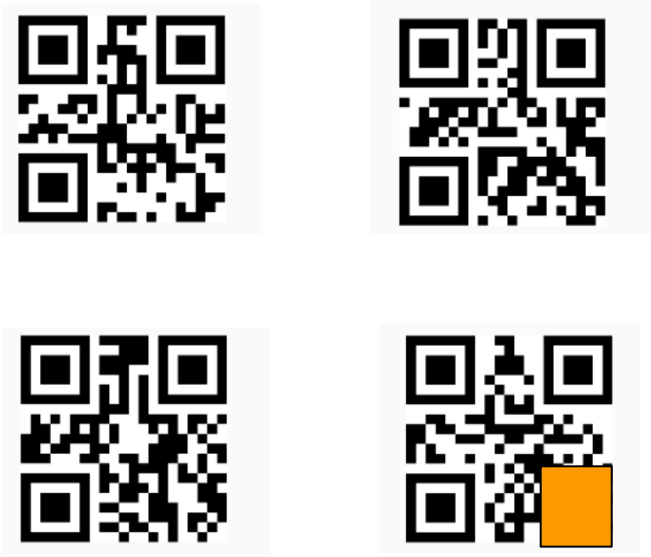
- 二维码有40个版本Version。Version 1是21 x 21的矩阵，Version 2是 25 x 25的矩阵，Version 3是29 x 29的矩阵，版本增加1，行列就会增加4。最高Version 40是177 x 177 的矩阵　　(40-1)*4+21 = 177　。
- 版本1的二维码最多可以储存25个字符或41个数字，而版本40的二维码最多可以储存4296个字符或7089个数字。
- 像素



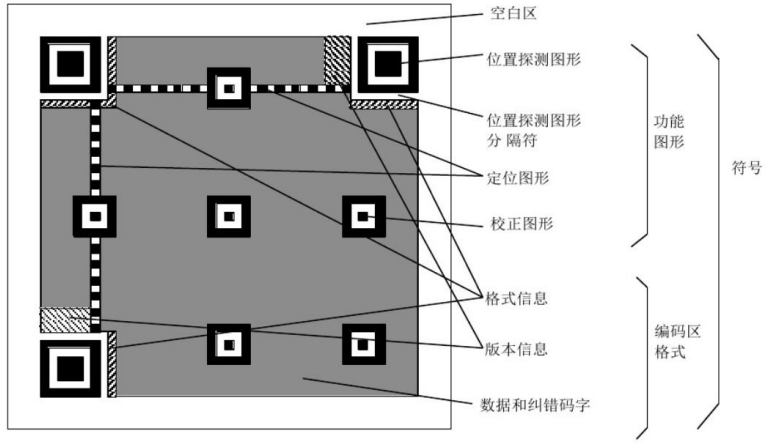
21 x 21

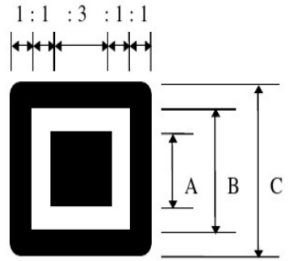


25 x 25



二维码结构





A: 3 模块
B: 5 模块
C: 7 模块

二维码图像包括功能区与数据区两部分。

- 功能区的作用是定位
  - 位置探测图形：由三个黑白相间的大正方形嵌套组成(7 x 7)，分别位于二维码左上角、右上角、左下角，目的是为了确定二维码的大小和位置。
  - 定位图形：由两条黑白相间的直线组成，便于确定二维码的角度，纠正扭曲。
  - 校正图形：由三个黑白相间的小正方形嵌套组成(5 x 5)，便于确定中心，纠正扭曲。
- 数据区包括数据、纠错码与版本信息。
  - 数据和纠错码：数据信息和相应的纠错码，纠错码可以保证当二维码的图像出现部分损失时，做到正确解码。
  - 版本信息：记录具体的版本信息（版本7以后需要这个编码）。
  - 格式信息：记录使用的掩码和纠错等级。

二维码数据编码

模式	指示符
ECI	0111
数字	0001
字母数字	0010
8位字节	0100
日本汉字	1000
中国汉字	1101
结构链接	0011
FNC1	0101（第一位置） 1001（第二位置）
终止符（信息结尾）	0000

版本	数字模式	字母数字模式	8位字节模式
1～9	10	9	8
10～26	12	11	16
27～40	14	13	16

二维码数据编码的过程

1）对存放的数据净荷进行分析，确定编码类型。二维码支持数字、字符、汉字等类型，也可以存放扩展的类型。
2）将净荷数据字符转换为比特流。每一块净荷数据前加一个模式指示符（编码类型），加长度字段，还要加上终止符。依据版本的要求可能在必要时，还要进行字段填充。
3）添加纠错编码。防止二维码图像出现部分损失时，无法提取数据。纠错有4种级别。
4）将上述数据和纠错码存放到数据区的存储空间。
5）添加格式信息、版本信息
6）进行掩码操作，实现二维码中黑白的均匀分布，生成二维码。

二维码数据编码的过程

1）对存放的数据净荷进行分析，确定编码类型。二维码支持数字、字符、汉字等类型，也可以存放扩展的类型。
2）将净荷数据字符转换为比特流。每一块净荷数据前加一个模式指示符（编码类型），加长度字段，还要加上终止符。依据版本的要求可能还要求在必要时，还要进行字段填充。

例：在版本1 对 01234567 进行数字编码，纠错级别是M

012 ->0000001100　345 ->0101011001　67 ->1000011

0000001100 0101011001 1000011，然后添加编码类型、长度字段、终止符，再按8bit补零

0001 0000001000 0000001100 0101011001 1000011 0000 000

二维码数据编码的过程

3）添加纠错编码。防止二维码图像出现部分损失时，无法提取数据。纠错有4中级别。通过RS算法生成纠错码。

错误修正容量	
L水平	7%的字码可被修正
M水平	15%的字码可被修正
[illegible]	[illegible]
[illegible]	[illegible]

版本1 M下需要128bits，不足最大bit的添加补齐码（11101100 00010001）

00010000 00100000 00001100 01010110 01100001 10000000--->

00010000 00100000 00001100 01010110 01100001 10000000 11101100 00010001 11101100 00010001 11101100 00010001 11101100 00010001 11101100 00010001

00010000 00100000 00001100 01010110 01100001 10000000 11101100 00010001 11101100 00010001 11101100 00010001 11101100 00010001 11101100 00010001----->

00010000 00100000 00001100 01010110 01100001 10000000 11101100 00010001 11101100 00010001 11101100 00010001 11101100 00010001 11101100 00010001 10100101 00100100 11010100 11000001 11101101 00110110 11000111 10000111 00101100 01010101

检错、纠错

- 二维码编码可以看作是一个通信报文。
- 通信报文需要具备检错、纠错能力。
- 检错就是在接收到通信报文后，能识别出是否有传输错误。
- 纠错就是在识别到有错误后，能够纠正错误。

纠错编码---先检错

常用的有CRC 循环冗余校核，以下图为例，在一次通信中，假设发送方要传送A、B、C、D信息，同时传送P信息，P为合计信息。 在接收方，分别对应接收的信息为A’、B’、C’、D’、P’，如果接收方进行 S 验算，就可以知道通信过程中是否有错误。

和验算法，假如有 A、B、C、D 四种商品的价格及合计金额。

	A	¥	100
	B	¥	200
	C	¥	300
	D	¥	400
合计	P	¥	1000

求校正子S（验算）

$S=A'+B'+C'+D'-P'=0$

（a）无错

	A	¥	100
	B	¥	300
	C	¥	300
	D	¥	400
合计	P	¥	1000

校正子

$S=A'+B'+C'+D'-P'=100$

（b）有错

图1 和验算法

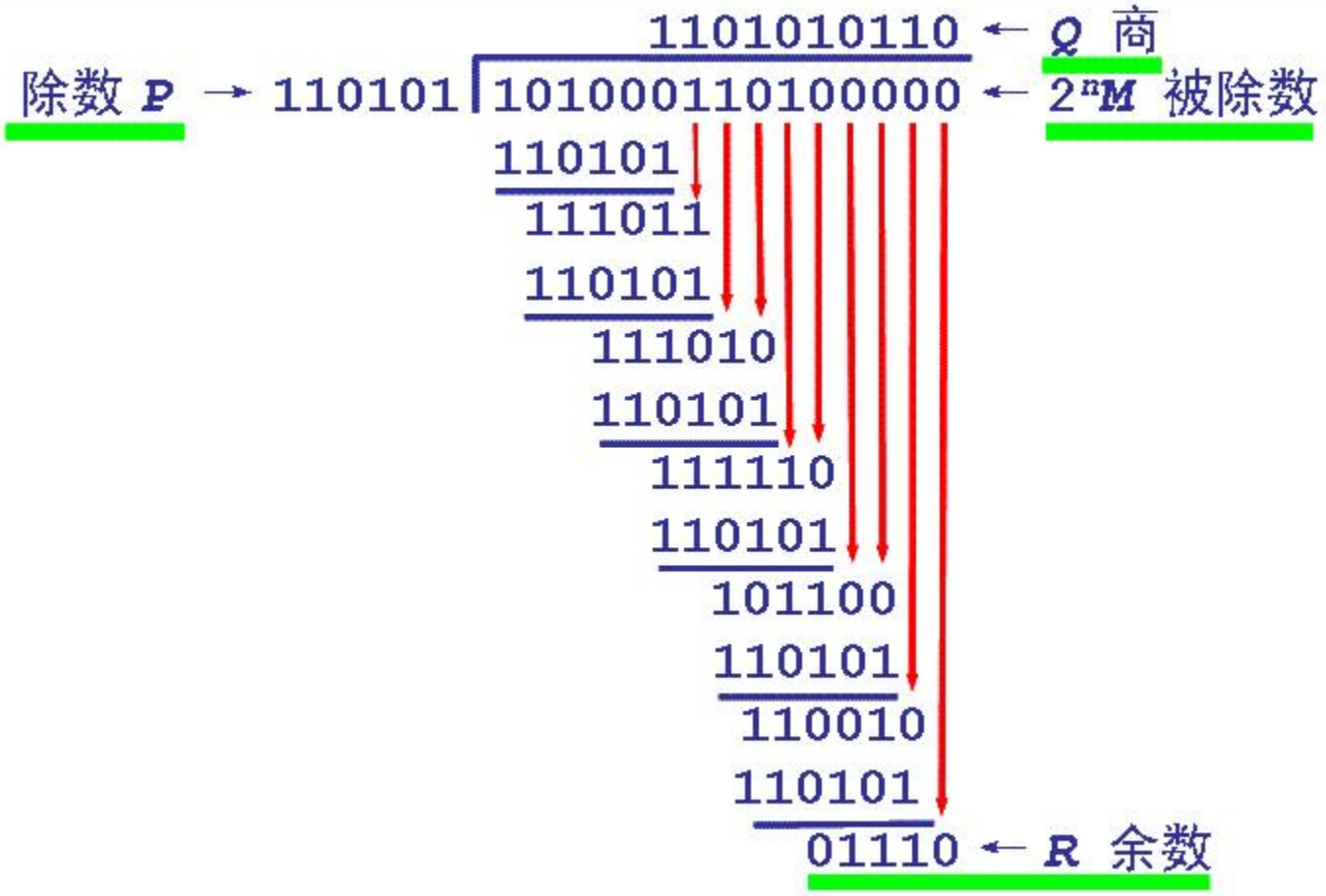
纠错编码---先检错

常用的有CRC 循环冗余校核 （Cyclic Redundancy Check）

设信息字段为K位，校验字段为R位，则码字长度为N(N=K+R)。设双方事先约定了一个R次多项式g(x)，则CRC码：$V(x)=A(x)g(x)=x^Rm(x)+r(x)$
其中： m(x)为K次信息多项式， r(x)为R-1次校验多项式。
这里r(x)对应的代码即为冗余码，加在原信息字段后即形成CRC码。

r(x)的计算方法为：在K位信息字段的后面添加R个0，再除以g(x) ，得到的余数即为r(x) (应为R－1位；若不足，而在高位补0)。

纠错编码---先检错



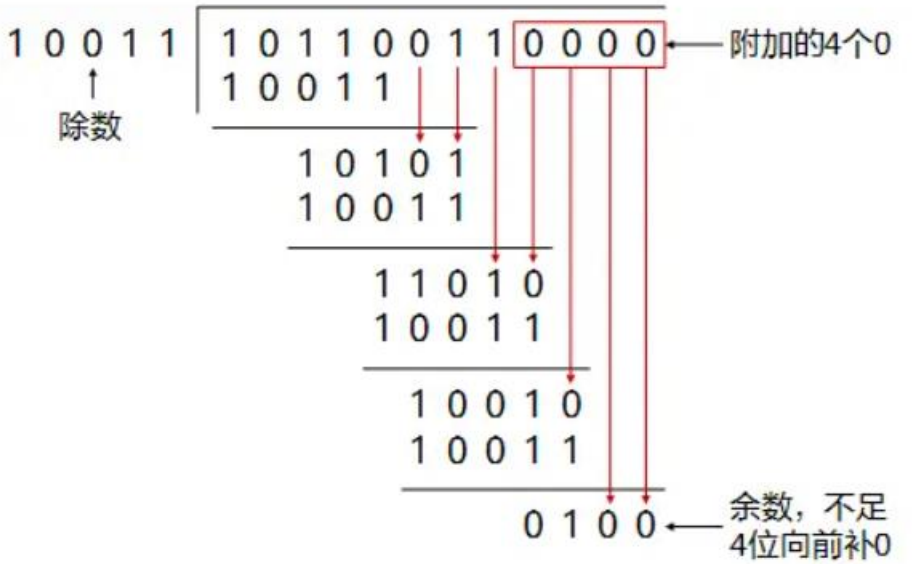
- 计算示例

➢ 设需要发送的信息为M = 1010001101，生成多项式g(x),即 P = 110101，R＝5。

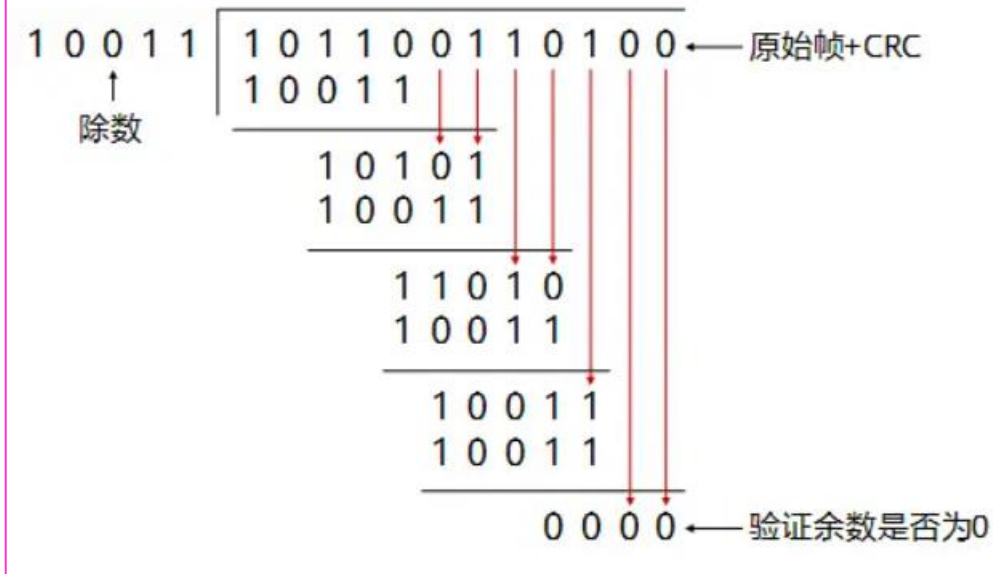
➢ 在M后加5个0，然后对P做模2除法运算，得余数r(x)对应的代码：01110。

➢ 故实际需要发送的数据是1010001101**01110**。

纠错编码---先检错



发送端CRC计算示例



接收端CRC校验示例

纠错编码---先检错

除数就是生成多项式

名称	多项式	表示法	应用
CRC-4	X^4+X^4+1	0X3	ITU-T G.704
CRC-8	X^8+X^2+X+1	0X07	ATM HEC, ISDN HEC
CRC-12	$X^{12}+X^{11}+X^3+X^2+X+1$	0X80F	telecom systems
CRC-16	$X^{16}+X^{15}+X^2+1$	0X8005	Bisync, Modbus, USB, ANSI X3.28, SIA DC-07, many others
CRC-CCITT	$X^{16}+X^{12}+X^5+1$	0X1021	X.25, V.41, HDLC FCS, XMODEM, Bluetooth, PACTOR, many others
CRC-32	$X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{12}+X^{11}+X^{10}+X^8+X^7+X^5+X^4+X^2+X+1$	0x04C11DB7	HDLC, IEEE 802.3 (Ethernet), SATA, ZIP, many others

常见生成多项式

纠错编码---先检错

还有什么时候需要检错，想想看

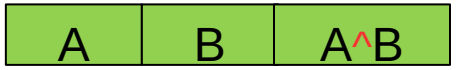
- 安装游戏软件后，“验完！”
- ZIP文件压缩
- 网络数据传输
- MD5
- 。。。

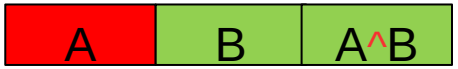
纠错编码---再纠错

- 纠错算法有很多，以常用的异或运算为例说明。

纠错编码---再纠错

- 在一次通信中，传输A、B两个数，为了保证传输可靠，同时传输 A^B，也就是在传输中，带上了冗余数据，除了传输A、B两个数，还要传输这异或 A^B，共传输3个数。



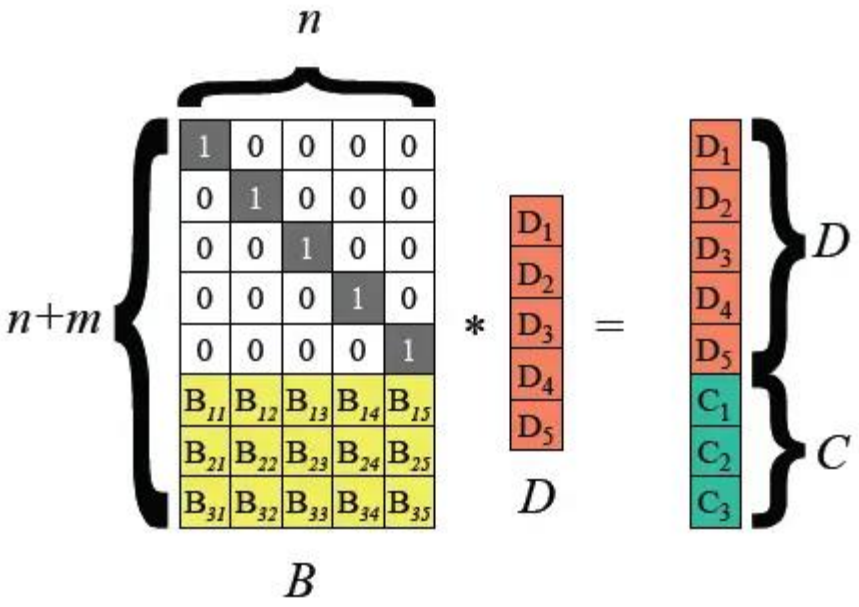


- 那现在想想，如果在传输中发生干扰出错，假设A出错了。接收方还能通过纠错获得A吗？

- 接收方只收到了B、A^B，但通过异或运算，
  B^ (A^B)=B^ (B^A)=(B^B)^A=0^A=A
  这样就恢复得到 A

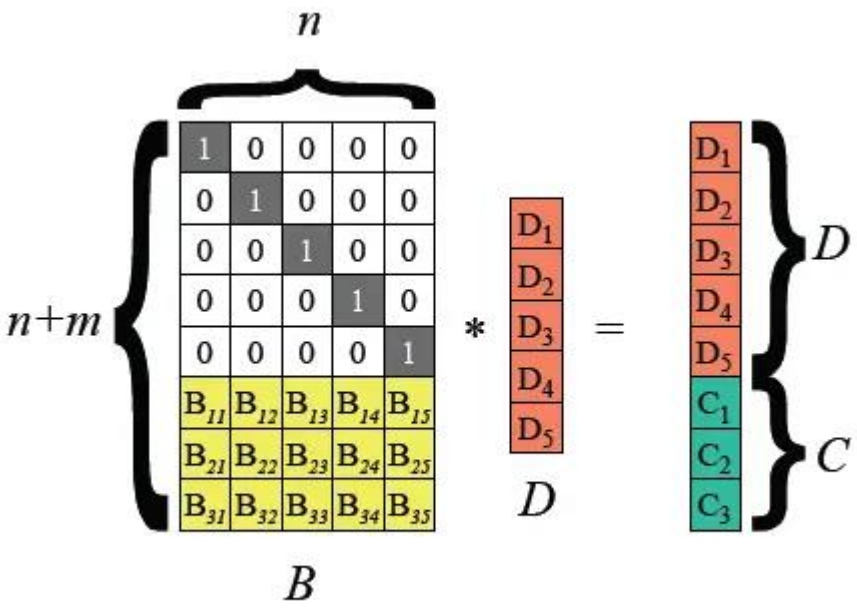
二维码纠错编码

里德-所罗门码（Reed-solomon codes，简称里所码或 RS codes）广泛用于各个领域，如RAID磁盘阵列，光盘，二维码等等。
RS code以字为编码解码单位，一般以8个二进制位或16个二进制位作为一个字（word）。将输入的数据当成是一个向量，如图：



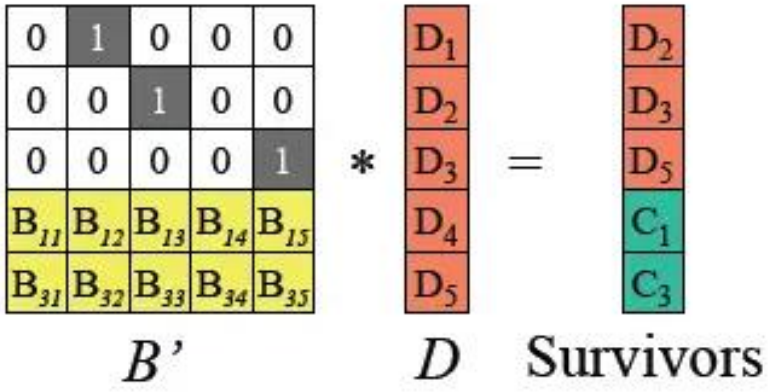
二维码纠错编码

- 图中，D_1,D_2,D_3,D_4,D_5 是原始数据，构成向量D=(D_1,D_2,D_3,D_4,D_5)。ReedSolomon的关键在于将左侧的矩阵生成出来，叫做编码矩阵（或称为生成矩阵、分布矩阵，Distribution Matrix），编码矩阵需要满足任意 n * n 大小的子矩阵可逆。
- 编码矩阵的上方都是单位阵（n行n列）,下方可以是范德蒙德矩阵或柯西矩阵。我们要传输的是矩阵B和向量D的乘积结果，即等式右边。



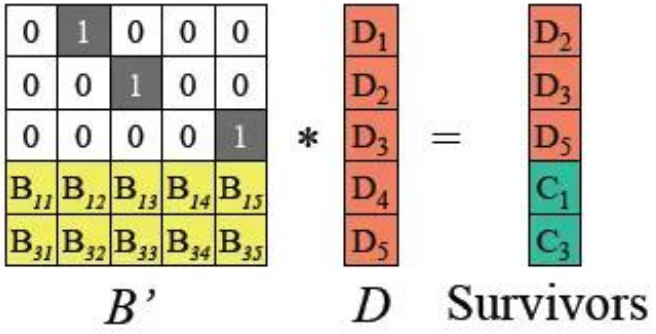
二维码纠错编码

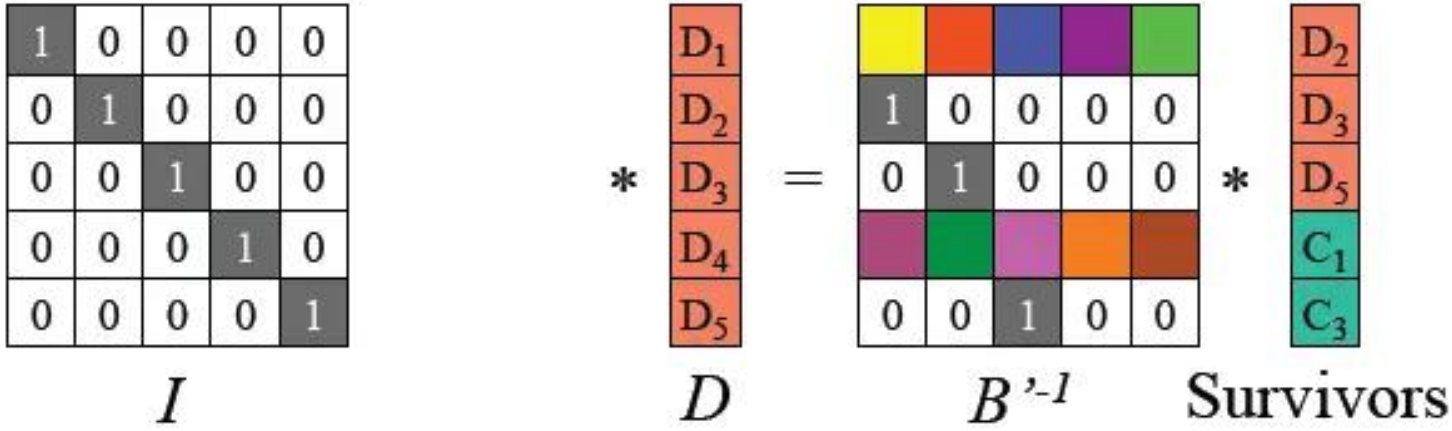
- 编码后的结果最多忍受m个数据块的错误。
- 将剩余正确的数据块对应行的编码矩阵取出来构成一个n*n 的子矩阵， 记为B’。
- 如图，survivors向量表示的是接收端收到的信息。（或者理解成D_1,D_4,C_2 丢包了），其对应的矩阵在左侧：



二维码纠错编码

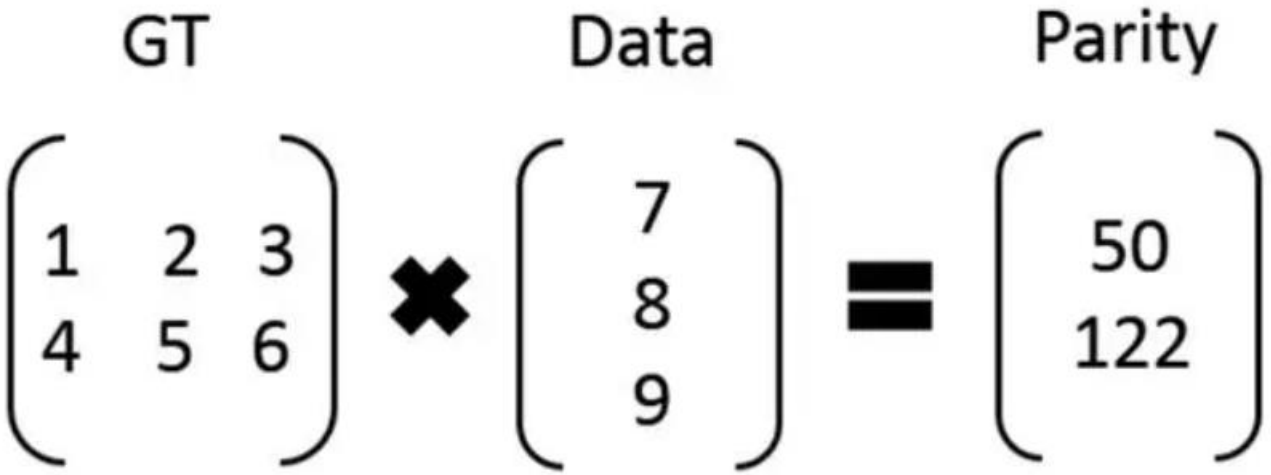
- 据矩阵的相关定理可知，求出B' 的逆矩阵 B'^{-1} ,可得$D = B'^{-1} * Survivors$





二维码纠错编码

比如：我们有 7、8、9 三个原始数据，通过矩阵乘法，计算出来两个校验数据 50、122。这时原始数据加上校验数据，一共五个数据：7、8、9、50、122，可以任意丢两个，然后通过算法进行恢复。



1*7+2*8+3*9 = 50

4*7+5*8+6*9 = 122

（1）x1 = 1

（2）x2 = 2

（3）x3 = 3

要知道x1，x2，x3三个数的值，只需要上面三个方程才可解出来。

（1）x1 = 1

（2）~~x2 = 2~~

（3）x3 = 3

（4）x1 + x2 + x3= 6

假设此时多了方程四，有趣的地方出现了，如果丢了一个方程，那么仍然可以用其他三个方程求出x1，x2, x3的值。相当于只多了一个方程就能解决x1,x2,x3任何一个数的值丢失的问题。

（1）x1 = 1

（2）x2 = 2

（3）x3 = 3

（4）x1 + x2 + x3= 6

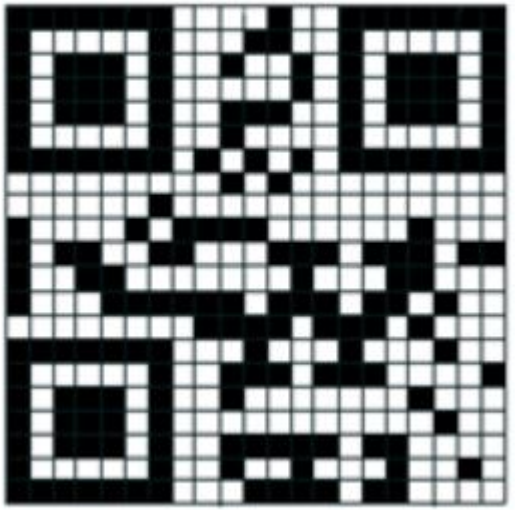
（5）x1 + 2*x2 +4*x3 = 17

（6）x1 + 3*x2 +9*x3 = 34

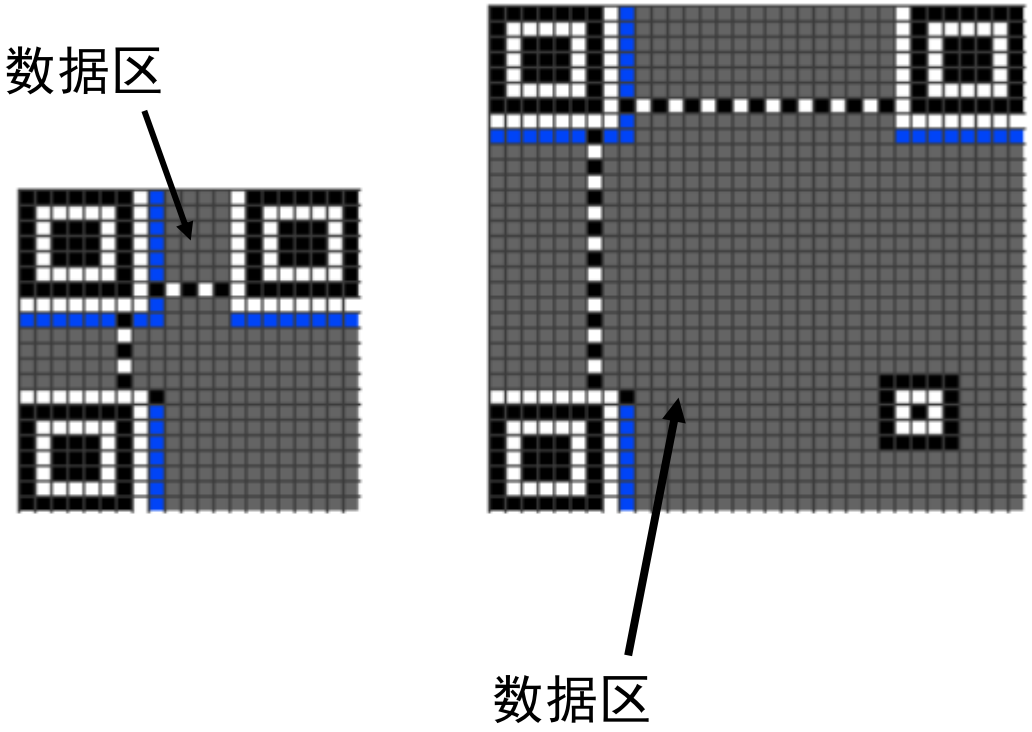
把上面的方程(1)(2)(3)看做是分布式系统的数据，（4）（5）（6）看做是code，那么只要一个code，即使丢了(1)(2)(3)中的任何一个数据都是可以恢复的， 达到这样的效果只需要存储4个方程。

如果采取副本策略，要达到（1）（2）（3）丢失任何一个数据都能恢复的话，只要把（1）（2）（3）三个方程都存储两份，也就是存储了6个方程。于是纠删码比副本策略在存储效率上的优势就体现出来。

二维码数据编码的过程

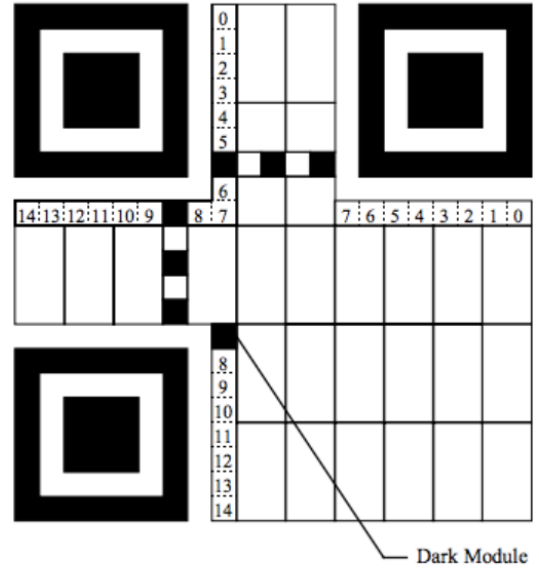


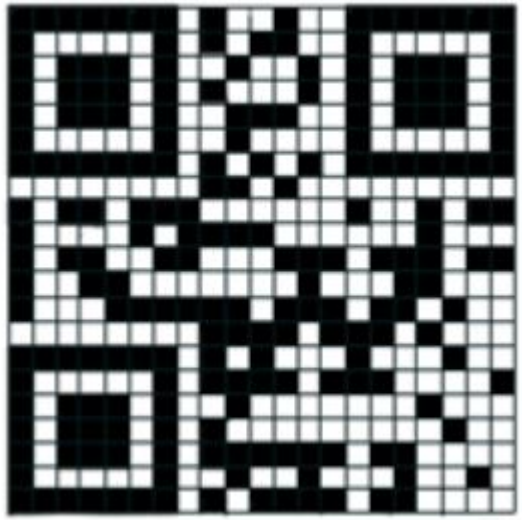
4）将上述数据和纠错码存放到数据区的存储空间。

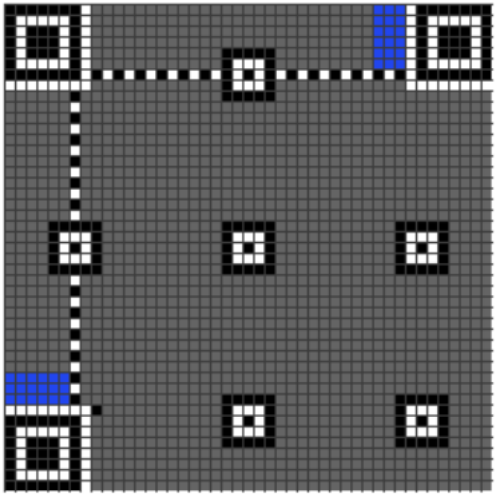


二维码数据编码的过程

5）添加格式信息、版本信息





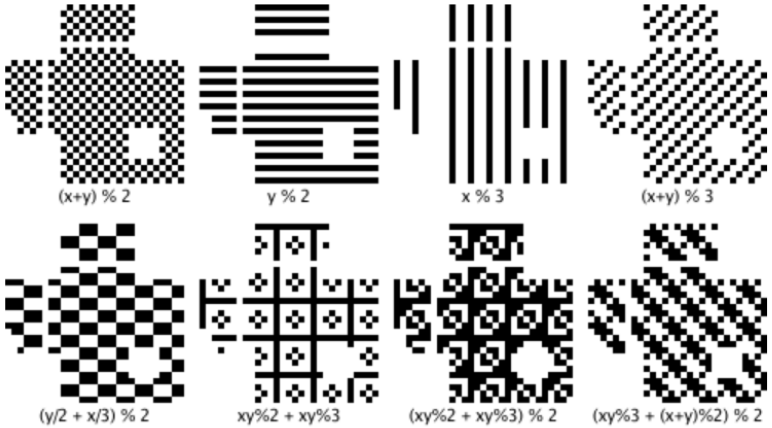


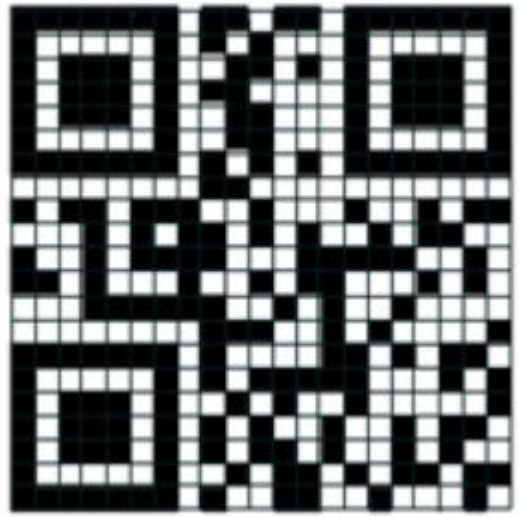
版本信息

二维码数据编码的过程

6）进行掩码操作。

掩码处理是为了避免数据区出现类似定位器形状的区域，或者出现大片空白等，可能会使扫描器混淆、错乱



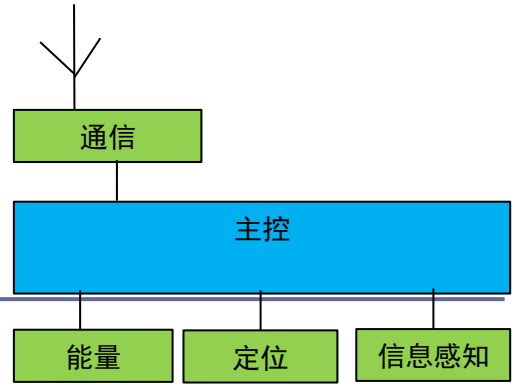


北京郵電大学
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

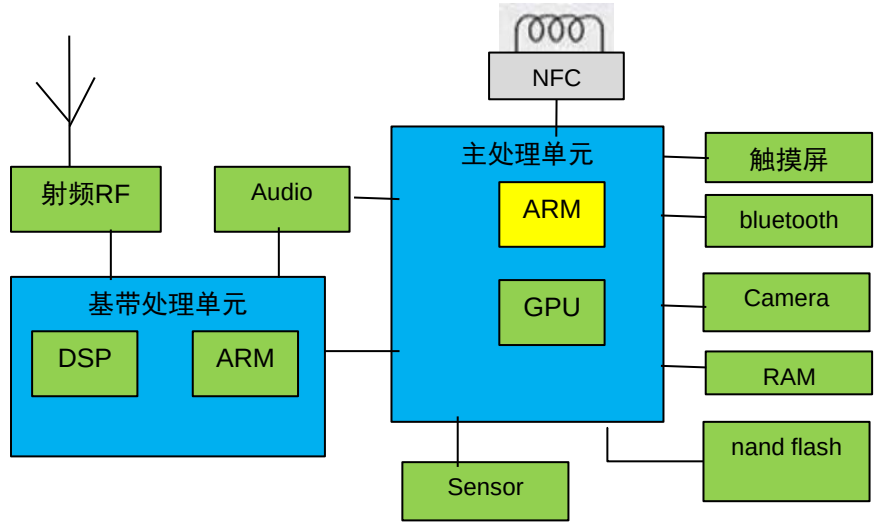
二维码解码的过程

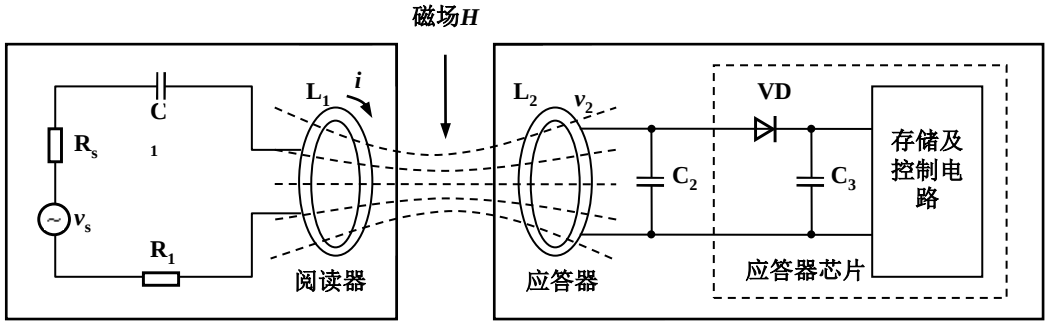
解码操作??

小结



- 移动互联网终端，能力各异
- 智能手机
- 自动识别技术
  - **NFC**
  - **RFID**
  - 二维码





北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

思考题

- 手机软解码视频与硬解码视频有什么区别?
- RFID技术与无线充电技术有啥联系?
- 移动支付一定要联网吗?
- 二维码安全吗?