虽有家财万贯 不如金卡傍身（六）

几种非接触式 IC 卡常用芯片及特性简介

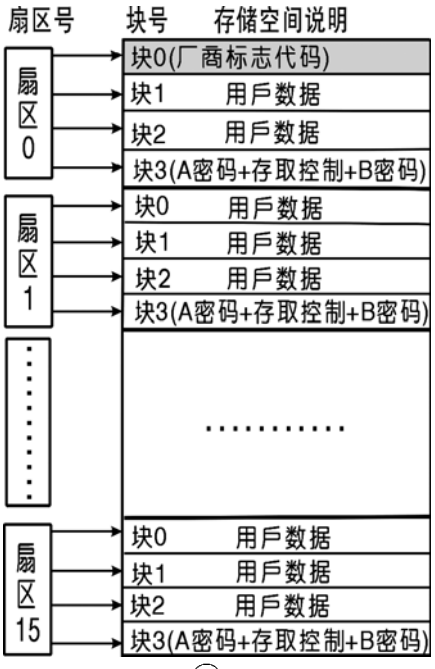
• 蔡凡弟 •

在智能卡家族中，非接触式 IC 卡因其具有高容量、高可靠（无机械触点和外物污染影响）、安全防伪、操作简单、寿命长（擦写次数高达 10 万次以上）等诸多优点，因而在更为广泛的应用场合中，非接触式 IC 卡越来越受到人们的重视。

世界上生产非接触式 IC 卡或其芯片的厂家很多，但其功能特性大都十分相近。在国内市面上公众较为常见的、用户使用量较多的多为飞利蒲公司的 MIFARE 系列、美国 TIMIC 公司的 E55XX 系列、瑞士礒M 公司的 H41XX 系列以及德国西门子公司的 R35S 系列等。因篇幅所限，以下简要介绍 MIFARE 1 及 E5551 芯片卡的主要功能特性。

一、MIFARE 芯片卡：

据报道，全世界使用菲利普 MIFARE 芯片的非接触式 IC 卡，约占同类智能卡销量的 60%以上。飞利蒲的 MIFARE 技术，已被制定为 ISO/IEC 14443 TYPE A、B、C、D 的国际标准。其它大型 IC 卡片或芯片制造商以及读写器制造商和软件应用开发商，大都以 MIFARE 技术为标准。进一步发展和推动了非接触式 IC 卡在各行业（特别是公共交通系统、消费支付系统、名片身份系统、门票管理系统等）中的广泛应用。



①

1、MIFARE 1 卡特点： MIFARE 标准卡目前已有 MF1、MF plus 以及 MF light 等多个版本。为便于介绍，这里主要依据 MF1 作简要介绍：

① MF1 IC 卡芯片采用先进的 CMOS 硅晶片制造工艺，内建高速 EEPROM 存储器、MCU 智能控制器等。卡片除了微型芯片 IC 及一个高效率天线外，无任何其它元件，见上期图 1。

② 卡片电路不用任何电池供电，工作时的能量由读写器天线发送频率为 13.56MHz 无线电载波信号，以非接触方式耦合到卡片天线上而产生电能，通常可达 2V 以上，见上期图 8。

③ 标准操作距离高达 10 cm（由 MF RC5XX 系列读写器芯片作核心模块）和 2.5cm（由 MF RC2XX 系列读写器芯片作核心模块），卡与读写器之间的通信速率高达 106K bit/s。

④ 具有先进的数据通信加密和双向密码验证功能，并且具有防冲突功能，可以在同一时间处理重叠在读写器天线有效工作距离内的多张卡片。

⑤ 其卡芯片在制造时具有全球唯一的序列号，没有重复相同的两张 MF 卡。

⑥ 内建 8K 位的 EEPROM 存储器。其空间被划分为可由用户单独使用的 16 个扇区。每区被分为 4 个数据存储块，每个块有 16 个字节（一字节为 8 位字长），其存储器结构见图 1。

⑦ 芯片设计有增 / 减值的专项数学运算电路，非常适合公共交通、地铁车站等行业的检票 / 收费系统，或充值钱包等多项目应用，其典型交易时间最长不超过 100ms。

⑧ 数据的擦写能力超过 10 万次以上，数据保存期大于 10 年，抗静电保护能力达 2KV。

2、MF1 IC 卡主要参数：

工作频率：13.56MHz	典型操作时间：≤96ms
读写距离：2.5—10cm	标准卡尺寸：85.6×54×0.8mm
存储容量：8K 位	存储类型：EEPROM
多重应用区：分 16 区	写卡周期：≥10 万次
读卡周期：无限	数据保存：≥ 10 年
操作温度：-20℃～+50℃	厂商序列号：32 位唯一
卡材料：PVC	

3、MF1 芯片结构： MIFARE 1 芯片内部结构较为复杂，它大致可分为射频接口和数字处理两大部分，这两部分的框图描述见图 2 所示。

②

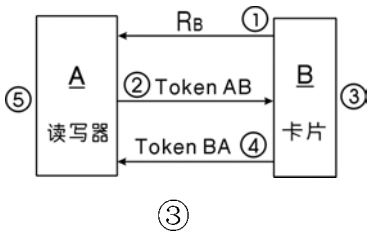
芯片的启动过程是：当卡天线在读卡器有效距离内而产生正弦波谐振时，其谐振电压经正弦波/方波转换电路变换后，分两路分别进入整流器和调制器。整流器输出直流电压经电压调节器控制后，直接向数字处理部分提供电能，从而使上电复位应答电路启动工作，同时接收由调制解调器送来的 RF 场时钟信号和向天线线圈传送经调制器处理后的复位应答信号。如果 RF 场中有多张卡，则处理过程会增加防冲突功能，若是单张卡，则直接进入选择启用以及与读写器之间进行相互三次认证，成功后，CPU 会启动存取控制器，对卡的交易内容进行读/写操作。

假如输入卡内的 RF 场时钟不正确（工作频率不对），或卡片的复位应答信号不能被读写器所辨别（读写器与卡片不配套），或虽然应答成功，但后面的三次相互认证失败（读写器与卡不属同一系统），其通信会出现暂停。其结果是用户取消刷卡交易，或者重新刷卡，以确定是否错误刷卡或卡片错用，通常使用者刷卡失败，如果排除蓄意非法刷卡外，一般为卡片错用所至。

4．MF1 的安全性能：非接触式 IC 卡的主要作用是让使用者能够非常方便、快捷、安全、完整地交换十分重要的用户信息。例如资金或身份等重要的数据信息。MF1 为了在交易过程中绝对不能有任何读、写方面的差错，在系统的每一张卡和读卡器之间，采用了三次不同方式的相互认证和访问条件的满足，才允许进入读写存取操作；另外，在存取操作中，还采用了多项措施来保证读写器与卡片之间的数据传送的完整性和可靠性。这是因为不完整的数据实质上就是错误数据，也就无“可靠”可言了。一旦出现不完整数据，读写过程停止。并且不能被存储在芯片中，其操作只能重新开始。其具体保证措施有如下六项：

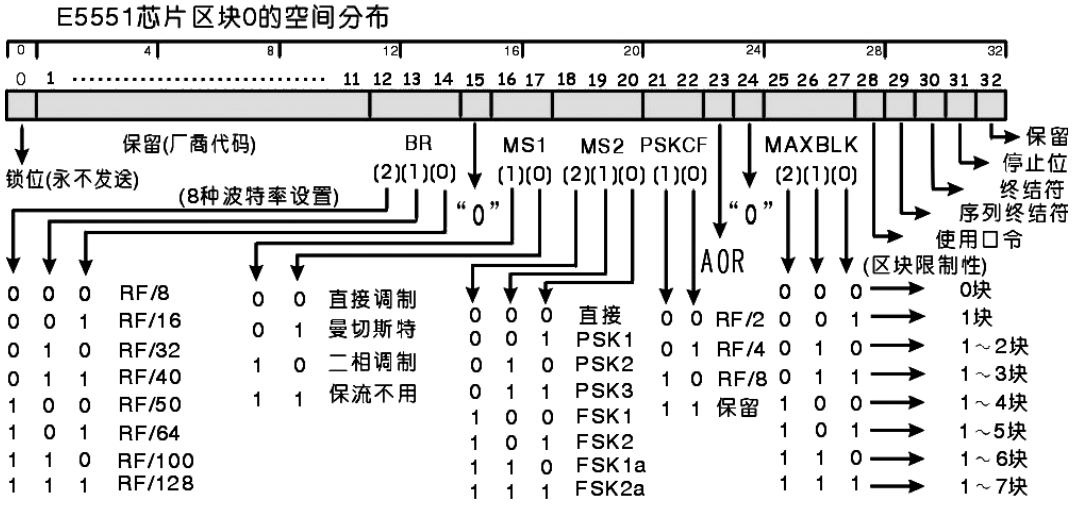
①设计有防冲突机制。②每个存储块有 16 位 CRC 纠错功能。③每一字节都有奇偶校验。④位数检查。⑤用位编码方式来区分信息的有无和“1”、“0”。⑥经由协议顺序及位流分析的信道监测。

为使信息传输中达到较高的保密水平，在信息被读写前必须经过三次不同内容的相互认证，另外还设置有对序列号的检查、访问密码及传输密码的保护、数据传递的加密等。也就是说卡片中的密码是受保护、不可读的，只有知道其密码的用户才能修改它。由存储器分区结构已知，每个扇区都有自己的访问密码，用户可根据各区的不同应用而设定不同的密码（一卡多用）。各区的访问密码又分别为 KEY A 和 KEY B 两组不同密码，依据访问条件，在分别校验 KEY A 和 KEY B 成功之后，才允许对存储器进行访问，通常，KEY A 用于存储器的减操作保护，KEY B 用于加操作保护。



③

图 3 示出了卡片信息在读写前的三次认证过程， 即卡片 B 在读写器 A 的 RF 场的有效区域内，① B 首先发出一个随机数 RB 给 A，② A 返回读写器标识符 AB 给 B，其标识符 AB 中，必需包含 B 的请求信息。③ B 收到标识符 AB 后，进行译码并验证标识符 AB 中所含的随机数 RB 是否与在①中所发出的一致。④ B 确认后，再次发给 A 一个标示符值 BA。⑤ 收到 BA 值后， A 译码并验证 RB 的正确性，同时还验证 BA 值中所含的随机数 RA 是否和②发出的一致。只有经过上述三次成功认证之后，才能进入访问条件操作（访问应用区密码和传输密码）。因它们受认证保护而不可随便读出，合法用户才能依访问条件而进入下一步信息数据的存取操作。由此可见，MF1 卡已具有很好的保密性能和安全地操作特性。再加之其容量大，可最多作 16 分区（或者说作 16 种不同用途）使用，是非接触式智能 IC 卡中较为优秀的电路之一。



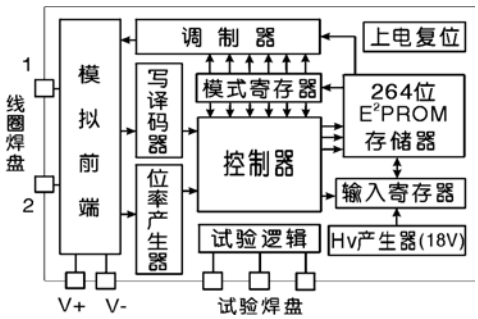
⑥

二、e5551 芯片卡

e5551 亦是非接触方式可读可写的识别 IC 芯片。适合 RF 在 125KHz 范围作一般用途使用。它与 MF 卡一样，也是由一个芯片和与之相连接的单组线圈构成应答卡片，线圈用作电路的电源供应和双向通信接口。

芯片设置有 264 位的 EEPROM 存储器，其空间被分为 8 个区块，每块有 33 位。读写设备可以按区块进行读写，区块根据需要也可以被保护起来。以防止重写而覆盖原有数据。8 个区块中，0 区块是专为设置 IC 的操作模式而保留的，被称为模式数据块，第 7 区块通常被用作口令存取块，以防止未经许可的擦写，如果不使用口令，该区块可以与 1～6 区块一样作为用户数据区块使用。

1、e5551 特性： ① 低功耗、低电压的高速 CMOS 识别 IC。② 非接触方式的电源供给以及数据的读写传输。③ 无线电波（RF）频率为 100KHz～150KHz，典型应用在 125KHz。④ 在每区块 33 位的 8 个区块内，共有 264 位 EEPROM 存储空间，实际可供用户存取数据使用的为 7 个区块的 224 位存储空间。⑤ 各区块具有写保护和扩展保护功能。⑥ 具有 AOR 请求应答功能，以防止多张卡同时进入有效的 RF 场而引起的读写冲突。⑦ 速度快，典型的写和验证一个区块时间≤50ms。 ⑧ BIN、FSK、



④

PSK、MANCHESTER 以及 BIPHASE 等多种数据调制模式可选。⑨以 RF 中心频率为参考点，其波特率(bit/s)可有 RF/8～RF/128 等几档选择。⑩ 可设置口令模式加载编程以及终结符模式加载区块。

2、E5551 芯片功能框图： 主要包括信号的模拟前端处理（电能的转换输入以及 RF 场时钟和接收数据的解调等）和后端以控制器、存储器为主的数据处理。见图 4 所示。

图 4 中下方的 5 个芯片焊盘，是作芯片功能测试之用的，当芯片测试正常后，通常用 VU 胶包封好不再使用。

3、e5551 的存储器分布： 见图 5 所示，其总体存储空间是 264 位，被分为 8 个区块，则每区块有 33 位。由于区块 0 被设置为模式数据区，它控制着整个芯片的各种操作或工作状态，用户是不能作存取使用的。另外，各区块“0”位是该区块的引导锁定位，亦不能被用户作数据区使用。因此，供用户数据使用的实际为 32 位的 7 个区块共 224 位的存取空间。如果要使用口令模式，则使用空间为 32 位的 6 个区块共 192 位，用户用 e5551 作一卡多用途显得空间不足，但作为某一特定用途，其存储空间还是足够使用的。

0 1 - 32 位

L	模式数据区块	区块0
L	用戶数据区块	区块1
L	用戶数据区块	区块2
L	用戶数据区块	区块3
L	用戶数据区块	区块4
L	用戶数据区块	区块5
L	用戶数据区块	区块6
L	用戶数据区块或口令保护区块	区块7

⑤

4、e5551 存储器的区块 0 结构： 见图 6 所示。由上述可知，区块 0 为模式数据区域，该区域内的各种模式数据控制着整个芯片的诸多功能，有兴趣的用户能够了解区块 0 的 33 位功能分布和设置，进一步提高使用效率和掌握使用技巧无疑是多有帮助的。

图中： 0 位为锁定位，1～11 位为生产厂商保留位，用于芯片厂商或卡片制造商的序列号空间，为只读特性。12～14 位（BR）为八种波特率设置，15 位和 24 位通常为“0”，否则将使芯片运行于独立分区的多功能状态。16～17 位（MS1）为调制段 1 的四种设置方式，18～20 位（MS2）为调制段 2 的八种设置方式，21～22 位为 PSK 时钟频率设置，23 位为请求回答，能自动判别和运行。25～27 位为大区块限制（MAXBLK）功能，主要应用于存储区够用或没必要对所有区块读写器操作时，可进行区块限制，以提高处理速度。如 MAXBLK 设置为“010”，则 E5551 只重复读取和传送 1-2 区块的数据，若设置为“000”，则只能读 0 区，而该区块大部分数据为隐，结果就只能读取厂商序列号。28 位为是否使用口令设置，若不使用，则区块 7 就可以作用户数据区使用。若使用口令，则块 7 被作为口令存取操作专用空间使用。29～30 位分别为序列终结符和区块终结符，它们是为数据编/译码的开始和结束作标记的特殊阻尼型式。31 位是停止位，低电平有效，是一个服从停止的标识符。32 位为厂商保留不用。（待续）

回目录 查看图表