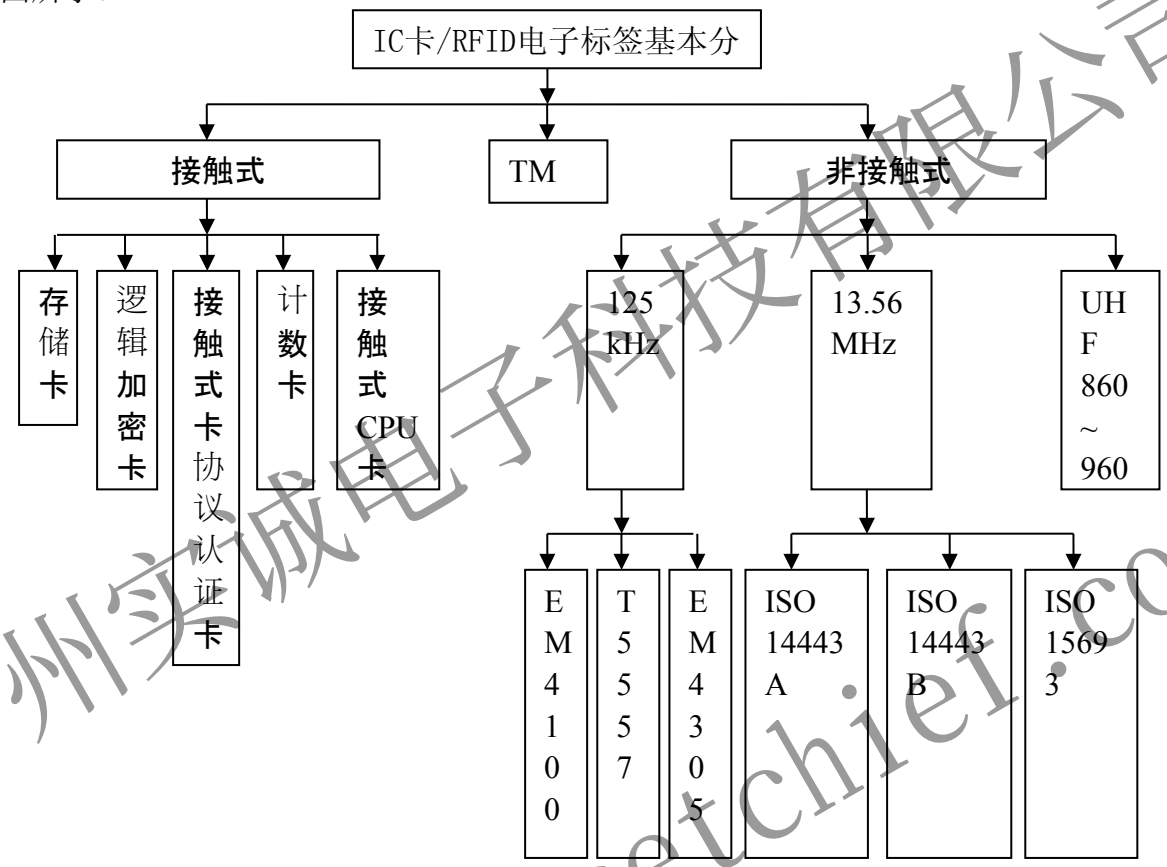
IC卡/RFID电子标签的分类识别与解密现状

广州实诚电子科技有限公司　　杨振野

IC卡/电子标签种类繁多，几乎所有的卡都是IC卡,常见的IC卡分类可如下图所示。



所谓RFID电子标签其实就是感应式IC卡,常见型号有MF0 （Ultra light）， MF1 (S50))， ICODE1，ICODE2， UHF。

无论是接触式还是非接触式的CPU卡，都具有极高的安全特性。如果没有设计缺陷，仅从外部攻击一般都是不可能成功的。

不同型号的IC卡可能具有相同的外观，所以并不能完全由来外观来确认型号。以下识别方式仅供参考。

1. 接触式IC卡类

接触式IC卡表面一定有镀金触点，使用时必须将卡插入卡座。

借助我司研发的**IC卡识别器**（99元），只需将卡插入即可识别出各种常见的接触式IC卡类型。当然，也可以借助各种IC卡读卡器（各地电脑城或电子城有售）来判定，只是比较麻烦而已。

这种卡多用于各种仪器的次数限制或权限限制，如门禁、速印机、美容仪器（电波拉皮、艾灸）等。

1.1存储卡

AT24C02，AT24C64等，可以采用**IC卡识别复制器**直接复制。

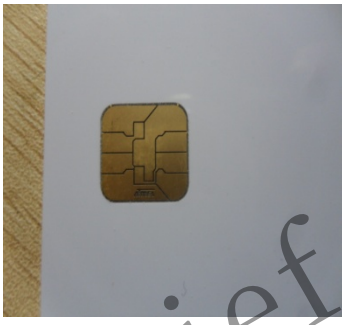
典型的存储卡触点

1.2 逻辑加密IC卡

常用型号如SLE4442/SLE5542，SLE4428，AT88SC102，AT88SC1604，AT88SC1604B，必须**先破解密码然后才可以复制**。

典型的4442触点

典型的4428触点



典型的AT88SC102触点

1.3 接触式CPU卡

对于接触式CPU卡，是不能直接复制的。要想解密，可以先采用**CPU卡数据记录分析仪分析其**读**写过程，分析可行性进而找出解决方案。**CPU卡具有极高的安全特性。如果没有设计缺陷，仅从外部攻击一般都不可能成功。如果存在设计缺陷，则可以采用模拟卡来解决。如果目的是发行与原卡一样的卡，则要求客户必须能够提供用卡设备，再按照**CPU卡数据记录分析仪的分析结果**尝试破解其全部密钥及设置。

2. 信息纽扣/TM卡/碰碰卡类

其特征是**端面一定是不锈钢的，且一般标有型号**，使用时必须将扣紧靠扣座。常见的型号如：DS1990/DS1990A(ID)，DS1991/DS1425（ID/多密钥/1KbitNVRAM），DS1982/DS1982U(ID, 1Kbit EPROM)，DS1985/DS1985U(ID,16Kbit EPROM)。这类卡由DALLAS公司出品，都具有全球唯一且不可更改的序列号（64bitROM）。


2.1 DS1990/DS1990A

64bitROM,多用于门锁和桑拿锁。由于其序列号不可改，所以只能采用微电脑芯片设计出模拟器来**模拟替代**。

2.2 DS1991

除具有64bitROM唯一序列号，还有三组密码。多用于激光设备的使用次数限制。对于DS1991必须先破解密码，然后才可以复制。破解出密码后，可以采用数据恢复的方法将其重复使用。由于唯一序列号的限制，按相同密码和数据复制出的DS1991不一定可用。对于这种情况，只需采用模拟替代扣就可以了。

2.3 DS1982/DS1982U，DS1985/DS1985U

为1Kbit EPROM，其数据只能将“1”写成“0”而不可逆转。多用于各种机加工或医疗设备的使用次数限制。这种扣虽然没有密码，但其数据都与其序列号相关联，所以直接采用DS1982复制出的新扣一定不能用，必须采用模拟替代扣。DS1985只是比DS1982容量大，破解方法类似。DS2502或DS2502U与DS1982功能相似；DS2505或DS2505U与DS1985相似；只是它们被封装成集成电路的样式了。

3. 125KHz

这种卡或标签多用于小区、楼宇、宾馆门卡或电子标签。特征是表面没有触点，多为异型扣或卡。如果是卡，可用强光由照射观察卡内的感应天线，其环形阴影宽度应大于3毫米。感应距离5厘米左右。

3.1 EM4100

常被称为ID卡，多用于小区楼宇门禁卡或扣。仅具有唯一序列号功能。现在可以采用T5557卡来复制替代。典型的EM4100外观如下所示，其表面有ID编码。

3.2 T5557/5567/5577/E5550

这种卡也具有不可复制的唯一序列号。可以设置成密码模式，也可以设置成无密码模式。

对于设置成密码模式的卡，只需采用T5557射频卡密码破解装置破解出密码后即可采用T5557射频卡快速抄卡器复制。

对于设置成密码模式的卡，由于其数据与其序列号有关联，所以不能直接复制。必须破解出其关联算法后才可以复制。只有极个别的门锁卡可以直接复制使用。

3.3 EM4305

与T5557卡类似，不再赘述。

4. 13.56MHz

这种卡或标签多用于小区、楼宇、宾馆门卡或电子标签。特征是表面没有触点，用强光由照射观察卡内阴影，环形感应天线阴影宽约为1毫米左右。感应距离5~10厘米左右。外观与上图一样，只是里面的感应天线不同。

4.1 MF0/ mifare ultralight

常被用作防伪标签。具有7字节唯一序列号和48字节数据存储区。对于这种卡，除非破解其关联算法，通常只能采用MF0模拟器复制模拟。

4.2 MF1/S50

共有16个扇区，每个扇区可存储48字节，且都设有6字节A/B密码。这种卡的UID一般是不能改写的，但现已有厂商可以提供UID可该写型兼容卡。

很多用卡系统采用了**一卡一密**的加密方式。即由每张卡的UID算出其密码。由于UID的唯一性，导致每张卡的密码均不相同，从而提高了破解难度。

由于厂家的设计缺陷，现在已有密码破解工具，仅有一张用卡即可破解。破解出密码后，即可用MF1-

S50型感应卡快速多功能16扇区读写器复制。如果16扇区的密码均未知，用通常的工具就不能测试出密码了。对于原装的mifare卡，仍然有一种密码破解16扇区全加密的工具，但这一工具对于国产的兼容卡无效。对于16扇区全加密的，还可以采用PM3工具截获通信数据后，借助专用软件分析出其中一个密码，然后再借助前述工具将全部密码解出。采用这种方法破解需要有用卡设备，且操作过程复杂，非专业人士操作的成功率只有50%。还有一种更专业的破解手段，即直接在接口芯片的引脚上截获数据，然后分析出密码。

4.3 ISO/IEC15693：ICODE1/ICODE2/TAG-IT（TI2048）

ICODE1、ICODE2和Tag-it都符合ISO/IEC15693协议，只是存储容量不同（分别是512 bits、1K bits和2K bits），一般都是作为RFID电子标签用于防伪。

对于ICDOE1，现已有能随意改写UID的ICODE1兼容标签。

对于ICODE2和Tag-it现在还没有能随意改写UID的ICODE2兼容标签。但可以按照客户要求订制特定UID的ICODE2兼容标签，一次订制不能少于15000片。

对于不同的应用需求，也可以制作出相应的模拟器。

5. UHF RFID

采用ISO18000-6C标准的超高频无源RFID电子标签，读写距离可达28米，多用于物流和防伪。中

国的UHF

RFID的可用频段为920~925MHz。这种标签具有唯一序列号、数据存储区和密码功能。