MW HRF 系列非接触式 IC 卡读写器

API 接口函数介绍

1.0 版

深圳市明华澳汉电子设备有限公司

目录

1 简介

1.1 本手册使用范围

本手册描述了非接触式 IC 卡读写器的使用及应用程序接口函数（API），所有 API 函数均可工作于 Windows 98、 Windows 2000、 Windows NT、 Windows XP 等操作系统上。

1.2 术语表和缩略语

CRC: 循环冗余校验
PCD: 近耦合设备
PICC: 近耦合集成电路卡
RWD: 读/写设备
AFI: 应用领域识别号
RFID: 射频识别号
VICC: 近距离集成电路卡
UID: 唯一识别号
DSFID: 数据保存格式识别号
RFU: 保留

1.3 概述

- 手册简介
- 读写器概述
- API 函数指南
- 通用函数
- 设备操作函数
- Mifare Standard 1K 卡片操作函数
- Mifare Standard 1K 卡片操作函数
- Mifare UltraLight 卡片操作函数
- Mifare Standard 4K 卡片操作函数
- 复旦 FM11RF005 卡片操作函数
- 华虹 SHC1102 卡片操作函数
- SAM/CPU 卡片操作函数
- MifarePro/Prox 卡片操作函数
- 附录（非接触卡特性）

2 读写器概述

HRF-35LT 是明华设备公司推出的又一款射频读写器。它采用了 USB 接口通讯和取电，支持 ISO14443-3 TypeA 协议的卡片，例如 Mifare One、UltraLight、Mifare 4K、MifarePro 等。随机提供的接口函数库可满足用户二次开发的需要；其完善、可靠的接口函数，支持访问射频卡的全部功能。

2.1 设备接口

USB 接口用于与上位 PC 联机通讯及设备取电；

2.2 读写器装箱清单

包装盒内配有：读写器，驱动光盘。

2.3 程序安装

运行 HRF_35LT.exe 按步骤安装我们的 HRF-35LT 软件开发包，安装结束后，在 c:下创建一个 MWHRF-35LT 的子目录，所有软件均在此目录下。

注：安装结束后，在 c:下创建一个 MWHRF-35LT 的子目录，所有软件均在此目录下。

2.4 软件

HRF-35LT 读写器软件包括：演示程序、函数库和应用范例

a. 演示程序

提供 Windows 版演示程序: DemoHRF 1.0.exe。

b. 函数库

WINDOWS32 位动态库

c. 应用范例

MWHRF-35LT\EXAMPLES 目录下提供各种开发平台的应用范例，包括 VB、DELPHI、VC 等。

2.5 技术指标

- 操作距离：HRF-35LT 为 35mm（Mifare 标准卡读写距离）
- 数据在卡和读写器之间传输时可进行数据加密和双向验证。（此项功能需要卡片的支持）
- 防冲突，可同时读取多张射频卡（此项功能需要卡片的支持）
- 功能操作：读、写、初始化值、加值、减值、读值和装载密码等（此项功能需要卡片的支持）
- 控制蜂鸣器鸣响功能
- 通讯接口：USB
- 工作频率 13.56MHZ
- 以 106kbit/s 速率高速访问射频卡
- 工作电源：USB 取电
- 环境温度：0° C～50° C
- 相对湿度：30%~95%
- 重量： 约 200 克
- 提供丰富的二次开发平台和应用范例

3 API 函数指南

3.1 软件开发包安装程序安装后主要目录和文件

软件开发包安装程序安装后 mwhrf-35lt 下的目录和文件：

Install.log	安装程序日志
Unwise.exe	卸载程序
Mwhrf-35lt\hrf-35lt\Demo.win\ DemoHRF1.0.exe	WINDOWS 下演示软件
\ mwrf32.dll	WINDOWS 32 位动态库
Mwhrf-35lt\hrf-35lt\Manual\hrf-35lt 中文使用手册.doc	
Mwhrf-35lt\hrf-35lt\API\	WINDOWS32 位动态库
Mwhrf-35lt\hrf-35lt\Examples\	VC，VB，DELPHI 等各种平台的范例

3.2 函数使用说明

函数调用应遵循如下规则：

（1）程序开始，首先要调用 rf_init( ) 函数打开读写器，建立读写器与 PC 之间的连接。

（2）用 rf_load_key()将卡中某一扇区密码输入到读写器中。如果使用直接密码认证，这步可以省略。

（3）调用 rf_card()函数或者连续调用 rf_request()、anticoll()、select()三个函数，成功可返回卡的序列号， 并且卡片进入激活状态。

（4）如果使用装载密码认证并且已装载密码，对于需要密码验证的卡片调用 rf_authentication()函数验证卡片的密码，一次只能验证一个扇区。
如果使用直接密码认证，则调用 rf_authentication_key()函数验证卡片的密码，用于验证的密码由函数参数中给定。

（5）对已验证过的扇区可进行读、写、初始化值、加值、减值等功能操作。对其它扇区的读、写操作必须重复上述（4）过程。

（6）由于高级函数集成了若干低级函数，所以调用前可不必运行（3）、（4）过程。

（7）对某张卡操作完成后，应用 rf_halt()函数结束对该卡的操作。

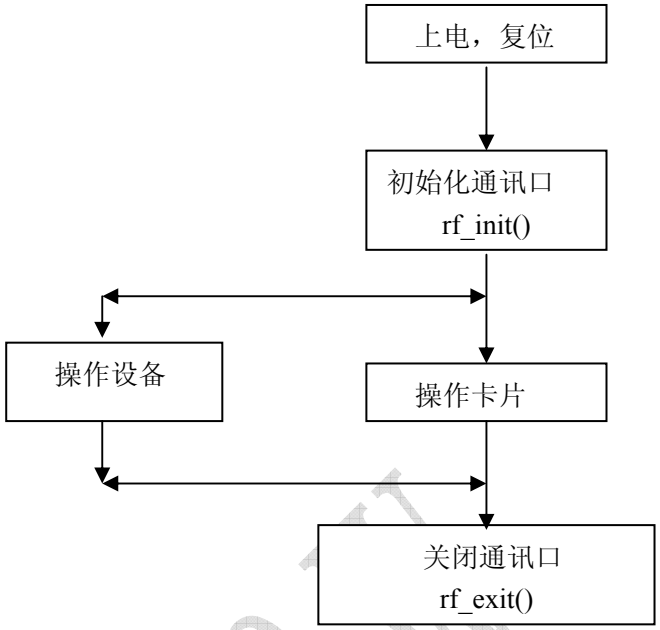
（8）程序正常退出或因错误退出之前，要用 rf_exit()函数关闭读写器，断开读写器与 PC 之间的连接；

（9）有关调用各种函数库的具体方法，请参考 mwhrf-35lt\hrf-35lt\Examples\目录下的使用范例。

4 库函数简介

本手册主要描述了 HRF-35LT 系列读写器的 API 函数，包括通用函数、设备操作函数和卡片操作函数。

HRF-35LT 系列读写器操作流程图



4.1 通用函数简介

通用函数用来实现打开/关闭串口、加密/解密以及16进制字符串和 ASCII 字符串间的相互转换等。

```
HANDLE   rf_init(__int16  port,long  baud);
int   rf_exit(HANDLE  icdev);
int   rf_decrypt(char *key,unsigned char *ptrSource,unsigned int msglen, char *ptrDest);
int   rf_encrypt(char *key,unsigned char *ptrSource, unsigned int msgLen,unsigned char
          *ptrDest);
int   hex_a(unsigned char *hex,char *a,unsigned char length);
int   a_hex(char *a,unsigned char *hex,unsigned char len);
```

4.2 设备操作函数

设备操作函数可以复位读写器、控制蜂鸣器、EEPROM 存储器、获取软件版本号、获取硬件版本号及产品系列号等。

复位 RF（射频）模块 module:

```
int   rf_reset(HANDLE icdev,unsigned __int16 _Msec);
```

控制蜂鸣器：

int rf_beep(HANDLE icdev,unsigned short _Msec);

获取硬件版本号:

int rf_get_status(HANDLE icdev,unsigned char *_Status);

获取产品系列号：

int rf_srd_snr(HANDLE icdev,__int16 lenth,unsigned char *rec_buffer);

获取软件版本号：

int lib_ver(unsigned char *str_ver);

4.3 复位 RF（射频）模块

复位射频模块函数将给射频模块断电几毫秒。射频模块复位后，所有在天线区域的卡片都回到上电复位状态。

int rf_reset (HANDLE icdev,unsigned __int16 _Msec);

功能: 将 RF（射频）模块的能量释放几毫秒

参数: icdev: rf_init()返回的设备描述符

_Msec: 复位时间 (0~ 500ms)

返回: =0: 成功

<>0: 出错

例: st=rf_reset (icdev,60);

4.4 卡片操作

卡片的应用程序接口（API）函数是根据卡片的标准来分类的：

4.4.1 Mifare 标准非接触卡操作函数

装载密码:

int rf_load_key (int icdev,unsigned char _Mode,unsigned char _SecNr,unsigned char *_NKey);

int rf_load_key_hex (int icdev,unsigned char _Mode,unsigned char _SecNr,char *_NKey);

低级和高级函数都可对 Mifare 卡进行同一操作。每一条高级函数都集成了一系列低级函数。这样用户使用起来会更方便。但是，如果对卡片进行多扇区或多块操作，速度将会变慢，因为在高级函数中许多低级函数的执行是重复的。在这种情况下，我们建议用户调用低级函数。

低级函数:

int rf_request(HANDLE icdev,unsigned char _Mode,unsigned __int16 *TagType);

int rf_anticoll(HANDLE icdev,unsigned char _Bcnt,unsigned long *_Snr);

int rf_select(HANDLE icdev,unsigned long _Snr,unsigned char *_Size);

int rf_authentication(HANDLE icdev,unsigned char _Mode,unsigned char _SecNr);

int rf_authentication_2(HANDLE icdev,unsigned char _Mode,unsigned char KeyNr,unsigned char Adr);

int rf_authentication_key(HANDLE icdev, unsigned char _Mode,unsigned char _BlockNr, unsigned char *_Key);
int rf_read(HANDLE icdev,unsigned char _Adr,unsigned char *_Data);
int rf_read_hex(HANDLE icdev,unsigned char _Adr, char *_Data);
int rf_write(HANDLE icdev,unsigned char _Adr,unsigned char *_Data);
int rf_write_hex(HANDLE icdev,unsigned char _Adr,char *_Data);
int rf_increment(HANDLE icdev,unsigned char _Adr,unsigned long _Value);
int rf_decrement(HANDLE icdev,unsigned char _Adr,unsigned long _Value);
int rf_restore(HANDLE icdev,unsigned char _Adr);
int rf_transfer(HANDLE icdev,unsigned char _Adr);
int rf_initval(HANDLE icdev,unsigned char _Adr,unsigned long _Value);
int rf_readval(HANDLE icdev,unsigned char _Adr,unsigned long *_Value);
int rf_decrement_transfer(HANDLE icdev,unsigned char Adr, unsigned long _Value);
int rf_halt(HANDLE icdev);

高级函数:

int rf_card(HANDLE icdev,unsigned char _Mode,unsigned long *_Snr);
int rf_changeb3(HANDLE icdev,unsigned char _SecNr,unsigned char *_KeyA,unsigned char _B0,unsigned char _B1,unsigned char _B2,unsigned char _B3,unsigned char _Bk,unsigned char *_KeyB);
int rf_check_write(HANDLE icdev,unsigned long Snr,unsigned char authmode,unsigned char Adr,unsigned char * _data);
int rf_check_writehex(HANDLE icdev,unsigned long Snr,unsigned char authmode,unsigned char Adr, char * _data);
int rf_HL_authentication(HANDLE icdev,unsigned char reqmode,unsigned long snr,unsigned char authmode,unsigned char secnr);
int rf_HL_decrement(HANDLE icdev,unsigned char _Mode,unsigned char _SecNr,unsigned long _Value,unsigned long _Snr,unsigned long *_NValue,unsigned long *_NSnr);
int rf_HL_increment(HANDLE icdev,unsigned char _Mode,unsigned char _SecNr,unsigned long _Value,unsigned long _Snr,unsigned long *_NValue,unsigned long *_NSnr);
int rf_HL_write(HANDLE icdev,unsigned char _Mode,unsigned char _Adr,unsigned long *_Snr,unsigned char *_Data);
int rf_HL_writehex(HANDLE icdev,unsigned char _Mode,unsigned char _Adr,unsigned long *_Snr, char *_Data);
int rf_HL_read(HANDLE icdev,unsigned char _Mode,unsigned char _Adr,unsigned long _Snr,unsigned char *_Data,unsigned long *_NSnr);
int rf_HL_readhex(HANDLE icdev,unsigned char _Mode,unsigned char _Adr,unsigned long _Snr, char *_Data,unsigned long *_NSnr);
int rf_HL_initval(HANDLE icdev,unsigned char _Mode,unsigned char _SecNr,unsigned long _Value,unsigned long *_Snr);

Mifare UltraLight 专用函数:

int rf_get_snr(HANDLE icdev,unsigned char *_Snr);

4.4.2 复旦 FM11RF005 非接触射频卡操作函数

装载密码函数:

int rf_load_key(int icdev,unsigned char _Mode,unsigned char _SecNr,unsigned char *_NKey);

int rf_load_key_hex(int icdev,unsigned char _Mode,unsigned char _SecNr,char *_NKey);

低级函数:

int rf_request(HANDLE icdev,unsigned char _Mode,unsigned __int16 *TagType);

int rf_anticoll(HANDLE icdev,unsigned char _Bcnt,unsigned long *_Snr);

int rf_select(HANDLE icdev,unsigned long _Snr,unsigned char *_Size);

int rf_authentication(HANDLE icdev,unsigned char _Mode,unsigned char _SecNr);

int rf_authentication_key(HANDLE icdev, unsigned char _Mode,unsigned char _BlockNr, unsigned char *_Key);

int rf_read(HANDLE icdev,unsigned char _Adr,unsigned char *_Data);

int rf_read_hex(HANDLE icdev,unsigned char _Adr, char *_Data);

int rf_write(HANDLE icdev,unsigned char _Adr,unsigned char *_Data);

int rf_write_hex(HANDLE icdev,unsigned char _Adr,char *_Data);

int rf_halt(HANDLE icdev);

高级函数:

int rf_card(HANDLE icdev,unsigned char _Mode,unsigned long *_Snr);

4.4.3 华虹 SHC1102 卡片操作函数

装载密码函数:

int rf_load_key(int icdev,unsigned char _Mode,unsigned char _SecNr,unsigned char *_NKey);

int rf_load_key_hex(int icdev,unsigned char _Mode,unsigned char _SecNr,char *_NKey);

低级函数:

int rf_request(HANDLE icdev,unsigned char _Mode,unsigned __int16 *TagType);

int rf_anticoll(HANDLE icdev,unsigned char _Bcnt,unsigned long *_Snr);

int rf_select(HANDLE icdev,unsigned long _Snr,unsigned char *_Size);

int rf_authentication(HANDLE icdev,unsigned char _Mode,unsigned char _SecNr);

int rf_authentication_key(HANDLE icdev, unsigned char _Mode,unsigned char _BlockNr, unsigned char *_Key);

int rf_read(HANDLE icdev,unsigned char _Adr,unsigned char *_Data);

int rf_read_hex(HANDLE icdev,unsigned char _Adr, char *_Data);

int rf_write(HANDLE icdev,unsigned char _Adr,unsigned char *_Data);

int rf_write_hex(HANDLE icdev,unsigned char _Adr,char *_Data);

int rf_halt(HANDLE icdev);

高级函数:

int rf_card(HANDLE icdev,unsigned char _Mode,unsigned long *_Snr);

4.4.4 SAM/CPU 卡操作函数

int rf_sam_rst(HANDLE icdev, unsigned char baud, unsigned char *samack);
int rf_sam_trn(HANDLE icdev, unsigned char *samblock,unsigned char *recv);
int rf_cpu_rst(HANDLE icdev, unsigned char baud, unsigned char *cpuack);
int rf_cpu_trn(HANDLE icdev, unsigned char *cpublock,unsigned char *recv);

4.4.5 MIFAREPRO 卡操作函数

int rf_request(HANDLE icdev,unsigned char _Mode,unsigned __int16 *TagType);
int rf_anticoll(HANDLE icdev,unsigned char _Bcnt,unsigned long *_Snr);
int rf_select(HANDLE icdev,unsigned long _Snr,unsigned char *_Size);
int rf_pro_rst(HANDLE icdev,unsigned char *_Data);
int rf_pro_trn(HANDLE icdev,unsigned char *problock,unsigned char *recv);
int rf_pro_halt(HANDLE icdev);

5 通用函数

下面将详细描述通用函数。

1) HANDLE rf_init (__int16 port,long baud)

功 能: 该函数用于建立读写器与 PC 机之间的连接，首先搜索无驱接口读写器，如果找到设备，则建立连接并返回。如果没有发现无驱接口读写器，则用选定的与 PC 机通讯的串口和波特率初始化读写器，这是操作读写器的第一步，这样可以获得通讯用的设备描述符供以后使用。

参 数: port: 通讯口号(0～250) ，对于无驱设备该参数无效
Baud: baudrate 通讯波特率(9600～115200)，对于无驱设备该参数无效

返 回: ≥0: 成功则返回设备描述符(≥0)
<0: 失败

例: int icdev;
icdev=rf_init(1,115200);// 波特率:115200,端口:com2

2) int rf_exit(HANDLE icdev);

功 能: 断开 PC 机与读写器之间的连接，并释放相关设备描述符。

参 数:
icdev: rf_init()返回的设备描述符

返 回: = 0: 成功
<>0: 失败

例: int st;
st=rf_exit(icdev);

3） int rf_encrypt(char *key,unsigned char *ptrSource, unsigned int msgLen,

unsigned char *ptrDest);

功 能: DES 算法加密。

参 数:

Key: 密钥，长度为 8个字节

ptrsource: 准备加密的明文,长度必须是8的倍数

msglen: 明文的长度，必须是8的倍数

ptrdest: 密文

返 回: = 0: 成功

<>0: 失败

例: //用 “12345678”加密 “abcdefghabcdefgh”

st=rf_encrypt(“1234567”,”abcdefghabcdefgh”,16,ptrdest);

4) int rf_decrypt(char *key,unsigned char *ptrSource,unsigned int msglen, char *ptrDest);

功 能: DES 算法解密。

参 数:

key: 密钥（必须和加密时的相同），长度为 8个字节

ptrsource: 密文

msglen: 密文的长度，必须是8的倍数

ptrdest: 明文

返 回: =0: 成功

<>0: 失败

例: //用 “12345678”来解密 “abcdefghabcdefgh”

st=rf_decrypt(“1234567”,”abcdefghabcdefgh”,16,ptrdest);

5) int hex_a(unsigned char *hex,char *a,unsigned char length);

功 能: 将 16 进制数转换为 ASCII 字符。

参 数:

hex: 16 进制数

a: 输出的 ASCII 字符

length: 16 进制数的长度

返 回: =0 成功

<>0 失败

6) int a_hex(char *a,unsigned char *hex,unsigned char len);

功 能: 将 ASCII 字符转换为 16 进制数。

参 数:

a : ASCII 字符

hex: 输出的 16 进制数

length: ASCII 字符的长度

返 回: =0 成功

<>0 失败

6 设备操作函数

1) int rf_reset(HANDLE icdev,unsigned __int16 _Msec);

功 能: 射频头复位(射频头掉电几毫秒)。

参 数:

icdev: rf_init()返回的设备描述符

_Msec: 复位时间，0～500毫秒有效

返 回: =0: 成功

<>0: 失败

例: st=rf_reset(icdev,60);

2) int rf_beep(HANDLE icdev,unsigned short _Msec);

功 能: 蜂鸣几毫秒。

参 数:

icdev: rf_init()返回的设备描述符

_Msec: 蜂鸣时间，单位：毫秒

返 回: = 0: 成功

<>0: 失败

例: st=rf_beep(icdev,10); //鸣叫10毫秒

3) int rf_get_status(HANDLE icdev,unsigned char *_Status);

功 能: 获取读写器的版本号。

参 数:

icdev: rf_init()返回的设备描述符

_Status: 返回读写器版本信息，长度为18字节

返 回: =0: 成功

<>0: 失败

例: int st;

unsigned char status[19];

st=rf_get_status(icdev,status);

4) int rf_srd_snr(HANDLE icdev,__int16 lenth,unsigned char *rec_buffer);

功 能: 获取读写器的产品序列号。

参 数:

icdev: rf_init()返回的设备描述符

length: 产品序列号的长度为16字节

receive_buffer: 返回的产品序列号

返 回: =0: 成功

<>0: 失败

例: unsigned char receive_buffer[17];

st=rf_srd_snr(icdev,16,receive_buffer);

5) int lib_ver(unsigned char *str_ver);

功 能: 获取 API 函数库版本号。
参 数:
strver: 返回 API 函数库版本号，长度为18个字节
返 回: =0: 成功
<>0: 失败
例： unsigned char str_ver[19];
st=lib_ver(str_ver);

6) int rf_gettime(HANDLE icdev,unsigned char *time);
功 能: 读取读写器的日期、星期和时间。
参 数:
icdev: rf_init()返回的设备描述符
receive_data: 接收数据, 长度大于7个字节
receive_data[0]: 年
receive_data[1]: 星期
receive_data[2]: 月
receive_data[3]: 日
receive_data[4]: 时
receive_data[5]: 分
receive_data[6]: 秒
返 回: =0: 成功
<>0: 失败
例: int st;
unsigned char datetime[8];
st=rf_gettime(icdev,datetime);
//datetime =“0x99,0x04,0x05,0x20,0x13,0x30,0x10”
//1999, Thursday, May 20, 13:30:10

7) int rf_settime(HANDLE icdev,unsigned char *time);
功 能: 设置读写器时钟的日期、星期和时间。
参 数:
icdev: rf_init()返回的设备描述符
time: 日期、星期和时间数据
time[0]: 年
time[1]: 星期
time[2]: 月
time[3]: 日
time[4]: 时
time[5]: 分
time[6]: 秒
返 回: =0: 成功
<>0: 失败
例: //设置日期为： 17/06/99 ，时间为：12:34:56, 星期一
unsigned char data[8];
data[0]=0x99;data[1]=0x1;data[2]=0x6;data[3]=0x17;

```
data[4]=0x12;data[5]=0x34;data[6]=0x56;
st=rf_settime(icdev,data);
```

8) int rf_gettimehex(HANDLE icdev,char *time);

功 能: 读取读写器时钟的日期、星期和时间 (16进制数)。

参 数:

icdev: rf_init()返回的设备描述符

receive_data: 返回的数据，长度大于14个字节

返 回: =0: 成功

<>0: 失败

例:
```
char data[15];
st=rf_gettimehex(icdev,data);
```

9) int rf_settimehex(HANDLE icdev,char *time);

功 能: 以16进制数设置读写器时钟的日期、星期和时间。

参 数:

icdev: rf_init()返回的设备描述符

time: 时间和日期的数值

返 回: =0: 成功

<>0: 失败

例:
```
//设置日期：17/06/99, 时间：12:34:56, 星期一
char data[14]="99010617123456";
st=rf_settimehex(icdev,data);
```

10) int rf_srd_eeprom(HANDLE icdev,__int16 offset,__int16 length, unsigned char *rec_buffer);

功 能: 读取 eeprom 的内容。

参 数:

icdev: rf_init()返回的设备描述符

offset: 位移地址 (0-249)

length: 数据长度(1-250)

recv_buffer: 接收数据的缓冲区

返 回: = 0: 成功

<>0: 失败

例:
```
unsigned char Send_buffer[250];
st=rf_srd_eeprom(icdev,0,200,send_buffer);
```

11) int rf_swr_eeprom(HANDLE icdev,__int16 offset,__int16 length,unsigned char *send_buffer);

功 能: 向 eeprom 中写入数据。

参 数:

icdev: rf_init()返回的设备描述符

offset: 位移地址(0-249)

length: 数据长度(1-250)

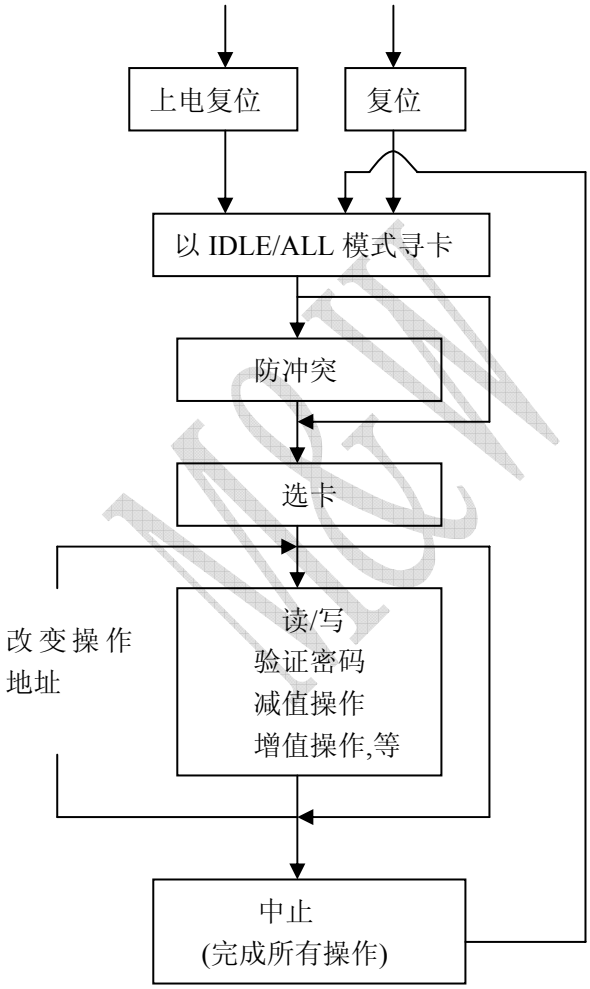
send_buffer: 将写入 eeprom 中的数据

返 回: = 0: 成功
<>0: 失败

例: unsigned char Send_buffer[249];
st=rf_srd_eeprom(icdev,0,250,send_buffer);

7 Mifare 标准非接触卡操作函数

7.1 Mifare 标准非接触卡操作流程图



7.2 认证方式比较

对于需要认证的卡片，这里有两种认证方式：装载密码认证和直接密码认证。下面比较这两种认证方式的优点和缺点。

a) 装载密码认证

优点：

- 安全性高

装载密码认证是指将密码下载到读写器存储单元，PC 机发送卡片认证指令后读写器从存储单元取出相应的密码进行卡片认证。由于密码下载到读写器存储单元后是不可读的，并且下载到读写器的密码在读写器断电后不会丢失，所以可以在安全的地方将密码下载到读写器，减少了密码在通讯过程中的传输次数。

- 装载密码可以和卡片交易分开，可以在不同的时间和地点进行。

缺点：

读写器密码存储单元有使用寿命，一般为十万次，如果装载过于频繁超过使用寿命，它将会坏掉不能再装载密码。

b) 直接密码认证的优点和缺点

优点：方便，没有使用寿命限制。

直接密码认证是指 PC 机向读写器发送卡片认证指令时将认证密码作为命令参数一起发送，直接使用参数中的密码对卡片进行认证。

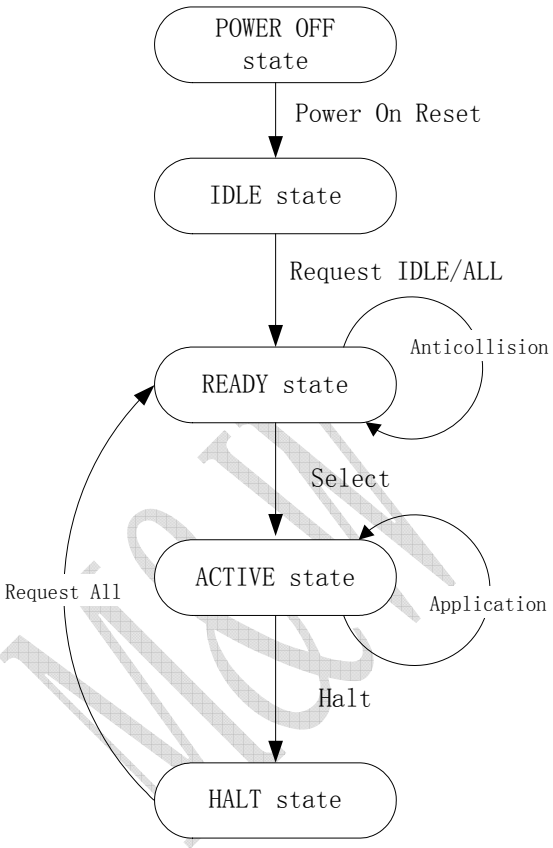
缺点：安全性不够

由于每次对卡片认证时，密码都会在通讯过程中传输，所以密码的安全性必须由应用商自己保证，通过其他方式来保证密码的安全性。

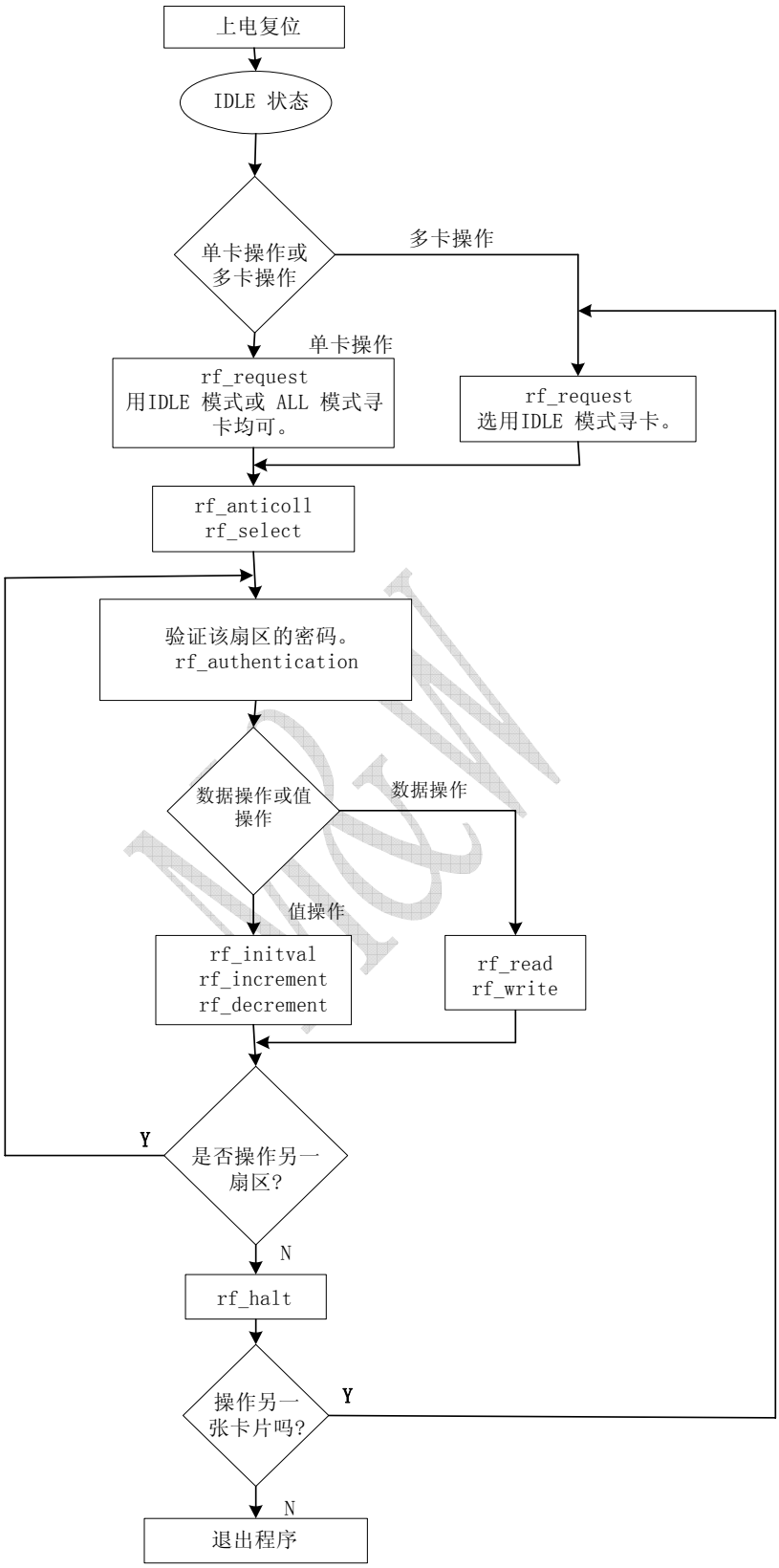
7.3 Mifare Standard 1K 卡片

这里详细介绍了 Mifare Standard 1K 卡片的操作函数，有关卡片的资料详见附录“Mifare Standard 1K”部分。

7.3.1 Mifare Standard 1K 卡片状态图



7.3.2 调用 Mifare Standard 1K 卡片 API 函数流程图



调用 Mifare std 1K 卡片 API函数流程图

7.3.3 操作函数说明

低级和高级函数都可对 Mifare 卡进行同一操作。每一条高级函数都集成了一系列低级函数。这样用户使用起来会更方便。但是，如果对卡片进行多扇区或多块操作，速度将会变慢，因为在高级函数中许多低级函数的执行是重复的。在这种情况下，我们建议用户调用低级函数。

int rf_load_key(HANDLE icdev,unsigned char _Mode,unsigned char _SecNr,unsigned char *_NKey);

功 能: 向读写器装载指定扇区的新密码（不与卡片进行通讯），读写器中有16个扇区的密码（0~15），每个扇区有两个密码(KEY A 和 KEY B)。

参 数:

icdev: rf_init()返回的设备描述符

_Mode: 密码类型

0 — KEY A

4 — KEY B

_SecNr: 须装载密码的扇区号(0～15)

_Nkey: 写入读写器的6字节新密码

返 回: = 0: 成功

<>0: 失败

例： // 装载扇区1的0号 key A：“a0a1a2a3a4a5”

unsigned char key[6]= {0xa0,0xa1,0xa2,0xa3,0xa4,0xa5 }

st=rf_load_key(icdev,0,1,key);

int rf_load_key_hex(HANDLE icdev,unsigned char _Mode,unsigned char _SecNr,char *_NKey);

功 能: 与 rf_load_key 函数相似。

参 数:

icdev: rf_init()返回的设备描述符

_Mode: 密码类型

0 — KEY A

4 — KEY B

_SecNr: 须装载密码的扇区号(0～15)

_Nkey: 写入读写器的6字节新密码

返 回: =0: 成功

<>0: 失败

例: //装载扇区1的0号 key A：“a0a1a2a3a4a5”

char key[ ]= “a0a1a2a3a4a5”;

st=rf_load_key_hex(icdev,0,1,key);

1) 低级函数

(1) int rf_request(HANDLE icdev,unsigned char _Mode,unsigned __int16 *TagType);

功 能: 该函数向卡片发出寻卡命令，开始选择一张新卡片时需要执行该函数。

参 数:

icdev: rf_init()返回的设备描述符

_Mode: 寻卡模式:

0 IDLE mode, 只有处在 IDLE 状态的卡片才响应读写器的命令。

1 ALL mode, 处在 IDLE 状态和 HALT 状态的卡片都将响应读写器的命令。

Tagtype: 返回卡片类型 (Mifare std. 1k: 0x0004, UltraLight: 0x0044, FM005: 0x0005, Mifare std. 4k: 0x0002, SHC1122: 0x3300)

返 回: =0: 成功

<>0: 失败

例：

```
unsigned char Mode=0;
unsigned int tagtype;
st=rf_request(icdev,Mode,&tagtype);
```

(2) int rf_anticoll(HANDLE icdev,unsigned char _Bcnt,unsigned long *_Snr);

功 能: 激活读写器的防冲突队列。如果有几张 MIFARE 卡片在感应区内，将会选择一张卡片，并返回卡片的序列号供将来调用 **rf_select** 函数时使用。

参 数:

icdev: rf_init()返回的设备描述符

_Bcnt: 预选卡片使用的位, 标准调用时为 bcnt=0.

_Snr: 返回的卡片序列号

返 回: = 0: 成功

<>0: 失败

例：

```
int st;
unsigned long snr;
st=rf_anticoll(icdev,0,&snr);
```

(3) int rf_select(HANDLE icdev,unsigned long _Snr,unsigned char *_Size);

功 能: 用指定的序列号选择卡片，将卡片的容量返回给 PC 机。

参 数:

icdev: rf_init()返回的设备描述符

_Snr: 卡片的序列号

_Size: 卡片容量的地址指针，目前该值不能使用

返 回: = 0: 成功
<>0: 失败

例: int st;
unsigned long snr=239474;
unsigned char size;
st=rf_select(icdev,snr,&size);

(4) int rf_authentication(HANDLE icdev,unsigned char _Mode,unsigned char _SecNr);

功 能: 验证读写器中的密码与需要访问的卡片的同一扇区(0~15)的密码是否一致。如果读写器中选择的密码（可用 **rf_load_key** 函数修改）与卡片的相匹配，密码验证通过，传输的数据将用以下的命令加密。

参 数:
icdev: rf_init()返回的设备描述符
_Mode: 验证密码类型：
0 — 用 KEY A 验证
4 — 用 KEY B 验证
_SecNr: 将要访问的卡片扇区号(0~15)

返 回: = 0: 成功
<>0: 失败

例： int st;
//authentication the 5th sector whit the 0^{th} key A
st=rf_authentication(icdev,0,5);

(5) int rf_authentication_2(HANDLE icdev,unsigned char _Mode, unsigned char KeyNr,unsigned char Adr);

功 能: 验证读写器中的密码与需要访问的卡片的同一扇区(0~15)的密码是否一致。如果读写器中选择的密码（可用 **rf_load_key** 函数修改）与卡片的相匹配，密码验证通过。主要用于验证扇区号大于15的扇区。

参 数:
icdev: rf_init()返回的设备描述符
_Mode: 验证密码类型：
0 — 用 KEY A 验证
4 — 用 KEY B 验证
KeyNr: 读写器中该扇区(0~15)的密码
Adr: 将要访问的卡片块号

返 回: = 0: 成功
<>0: 失败

例: 用读写器中0扇区的 KEY A 验证块2。
int st;
st=rf_authentication_2(icdev,1,0,2);

(6) int rf_authentication_key(HANDLE icdev, unsigned char _Mode, unsigned char _BlockNr, unsigned char *_Key);

功能: 利用函数参数中提供的密码对卡片指定数据块进行认证。如果参数中提供的

密码与卡片的密码匹配，则认证成功，反之则认证失败。

参数:

icdev: rf_init()返回的设备描述符

_Mode: 验证密码类型：

0 — 用 KEY A 验证

4 — 用 KEY B 验证

BlockNr: 卡片数据块地址(0~63)

_Key: 用于卡片认证的密码

返回: = 0: 正确

<>0: 错误

例:
```
unsigned char key[] = {0xff, 0xff, 0xff, 0xff, 0xff, 0xff};
st=rf_authentication_key(icdev, 0, 0, key);
```

(7) int rf_read(HANDLE icdev,unsigned char _Adr,unsigned char *_Data);

功 能: 从一张选定并通过密码验证的卡片读取一块共16个字节的数据。

参 数:

icdev: rf_init()返回的设备描述符

_Adr: 读取数据的块号(0~63)

_Data:读取的数据，PC 机上 RAM 的地址空间由调用该函数来分配。

返 回: = 0: 成功

<>0: 失败

例:
```
int st;
unsigned char data[16];
st=rf_read(icdev,1,data);
```

(8) int rf_read_hex(HANDLE icdev,unsigned char _Adr, char *_Data);

功 能: 读取16进制数的16 个字节。

参 数:

icdev: rf_init()返回的设备描述符

_Adr: 块地址, 0~63

_Data: 读取的数据

返 回: =0: 成功

<>0: 失败

例:
```
int st;
unsigned char data[32];
//read data from block 1
st=rf_read_hex(icdev,1,data);
```

(9) int rf_write(HANDLE icdev,unsigned char _Adr,unsigned char *_Data);

功 能: 将一块共16字节写入选定并验证通过的卡片中。

参 数:

icdev: rf_init()返回的设备描述符

_Adr: 写入数据的块地址 (1~63)

_Data: 写入数据,长度为16字节

返 回: =0: 成功
<>0: 失败
例: int st;
unsigned char data[16]={0x00,0x11,0x22,0x33,0x44,0x55,0x66,0x77,
0x88,0x88,0x77,0x66,0x55,0x44,0x33,0x22,0x11};
st=rf_write(icdev,1,data); // 写入块1

(10) int rf_write_hex(HANDLE icdev,unsigned char _Adr,char *_Data);

功 能: 以十六进制写数据, 一次必须写一个块。
参 数:
icdev: rf_init()返回的设备描述符
_Adr: 写入数据的块地址 (1~63)
_Data: 写入数据,长度为32字节
返 回: =0: 成功
<>0: 失败
例: int st;
unsigned char data[32]="a1a2a3a4a5a6a7a8a1a2a3a4a5a6a7a8";
st=rf_write_hex(icdev,1,data); //write block 1

(11) int rf_initval(HANDLE icdev,unsigned char _Adr,unsigned long _Value);

功 能: 初始化某一块的值。
参 数:
icdev: rf_init()返回的设备描述符
_Adr: 块地址
_Value: 初始化的目标值
返 回: =0: 成功
<>0: 失败
例: int st;
unsigned long value=1000;
st=rf_initval(icdev,1,value);

注：对某一块进行值操作时使用的是特殊的数据结构，所以需要进行初始化，然后才可以进行其它的增值和减值操作。

(12) int rf_increment(HANDLE icdev,unsigned char _Adr,unsigned long _Value);

功 能: 对值操作的块进行增值操作。
参 数:
icdev: rf_init()返回的设备描述符
_Adr: 值操作的块地址
_Value: 增加的值
返 回: = 0: 成功
<>0: 失败
例: int st;
unsigned long value=2;

```
st=rf_increment(icdev,1,value);
```

(13) int rf_decrement(HANDLE icdev,unsigned char _Adr,unsigned long _Value);

功 能: 对值操作的块进行减值操作。

参 数:

icdev: rf_init()返回的设备描述符

_Adr: 值操作的块地址

_Value: 减少的值

返 回: =0: 成功

<>0: 失败

例:

```
int st;
unsigned long value=2;
st=rf_decrement(icdev,1,value);
```

(14) int rf_readval(HANDLE icdev,unsigned char _Adr,unsigned long *_Value);

功 能: 读出指定值操作块的当前值。

参 数:

icdev: rf_init()返回的设备描述符

_Adr: 值操作的块地址

_Value: 返回读出的值操作块的内容

返 回: = 0: 成功

<>0: 失败

例:

```
int st;
unsigned long value;
//read the content and putin value
st=rf_readval(icdev,1,&value);
```

(15) int rf_restore(HANDLE icdev,unsigned char _Adr);

功 能: 将某块的数据传入卡的内部寄存器中。

参 数:

icdev: rf_init()返回的设备描述符

_Adr: 卡片上将读出数据的块地址

返 回: =0: 成功

<>0: 失败

例:

```
int st;
st=rf_restore(icdev,1);
```

注：用此函数将某一块内的数值传入卡的内部寄存器，然后用 rf_transfer()函数将寄存器的数据再传送到另一块中去，即实现了块与块之间的数值传送。

(16) int rf_transfer(HANDLE icdev,unsigned char _Adr);

功 能: 将内部寄存器的数据传送到某一块中。进行此项操作必须验证该扇区的密码，在执行 increment, decrement 或 restore 操作后可直接调用。

参 数:

icdev: rf_init()返回的设备描述符
_Adr: 内部寄存器的内容将存放的地址。.

返 回: =0 : 成功
<>0: 失败

例: int st;
st=rf_transfer(icdev,1);

(17) int rf_decrement_transfer(HANDLE icdev,unsigned char Adr, unsigned long _Value);

功 能: 通过传送来减少块的值。

参 数:

icdev: rf_init()返回的设备描述符
_Adr: 块地址
_Value: 减少的值

返 回: =0: 成功
<>0: 失败

例: int st;
unsigned long value=2;
st=rf_decrement_transfer(icdev,1,value);

(18) int rf_halt(HANDLE icdev);

功 能:将一张选中的卡片设为“Halt”模式，只有当该卡再次复位或用 ALL 模式调用 request 函数时，读写器才能够再次操作它。

参 数:

icdev: rf_init()返回的设备描述符

返 回: =0: 成功
<>0: 失败

例: st=rf_halt(icdev);

注 ： 使用 rf_card()函数时，如果模式选择为 0 则在对卡进行读写操作完毕后，必须执行 rf_halt()，且只能当该卡离开并再次进入操作区域时，读写器才能够再次操作它。

2) 高级函数

(19) int rf_card(HANDLE icdev,unsigned char _Mode,unsigned long *_Snr);

功 能: 寻卡并返回卡片的系列号，它可以完成低级函数 rf_request, rf_anticoll 和 rf_select 的功能。

参 数:

icdev: rf_init()返回的设备描述符
_Mode: 寻卡模式
0: IDLE 模式，一次只操作一张卡
1: ALL 模式，一次可操作多张卡
_Snr: 返回卡片的系列号

返 回: =0 : 成功
<>0 : 失败

例:
```
int st;
unsigned char Mode=0; //IDLE mode
unsigned long snr;
st=rf_card(icdev,Mode,&snr);
```

注：rf_card()是三个低级函数的组合:rf_request(),rf_select() 和 rf_anticoll()。
注意：选用 IDLE 模式寻卡时，完成对卡片的操作后调用 rf_halt 函数来停止操作，此后读写器不能找到卡片，除非卡片离开操作区域并再次重新进入。

选用 ALL 模式寻卡时，完成对卡片的操作后调用 rf_halt 函数来停止操作，此后读写器仍能找到该卡片，无须离开操作区域并再次重新进入。

(20) int rf_changeb3(HANDLE icdev,unsigned char _SecNr,unsigned char *_KeyA,unsigned char _B0,unsigned char _B1,unsigned char _B2,unsigned char _B3,unsigned char _Bk,unsigned char *_KeyB);

功 能: 修改 KeyA, 访问条件和 KeyB.

参 数:

icdev: rf_init()返回的设备描述符
_SecNr: 扇区号
_KeyA: key A
_B0: 0块的控制位，低三位（D2D1D0）对应为 C10,C20,C30.
_B1: 1块的控制位，（D2D1D0）对应为 C11,C21,C31
_B2: 2块的控制位，（D2D1D0）对应为 C12,C22,C32
_B3: 3块的控制位，（D2D1D0）对应为 C13,C23,C33
_Bk: 保留参数,设为0.
_KeyB: key B

返 回: =0: 成功
<>0: 失败

例:
```
int st;
unsigned char keya[6]={0xa0,0xa1,0xa2,0xa3,0xa4,0xa5};
unsigned char keyb[6]={0xb0,0xb1,0xb2,0xb3,0xb4,0xb5};
st=rf_changeb3(icdev,keya,0x04,0x04,0x04,0x04,0,keyb);
```

(21) int rf_check_write(HANDLE icdev,unsigned long Snr,unsigned char authmode,unsigned char Adr,unsigned char * _data);

功 能: 检查写入卡片的内容，在执行 rf_write () 函数后调用该函数。

参 数:

icdev: rf_init()返回的设备描述符
Snr: 卡片系列号
Authmode: 密码验证模式
0 用 A 密码验证
1 用 B 密码验证
Adr: 块地址

_data: 检查的内容.

返 回: =0: 成功

<>0 失败

例： unsigned char databuff[]={0x00,0x11,0x22,0x33,0x44,0x55,0x66,
0x77,0x88,0x88,0x77,0x66,0x55,0x44,0x33,0x22,0x11};
unsigned char authmode=0;
st=rf_write(icdev,4,databuff); // 写入第4块
st=rf_check_write(icdev,authmode,4,databuff); // 检查第4块的内容正确与否

(22) int rf_check_writehex(HANDLE icdev,unsigned long Snr,unsigned char authmode,unsigned char Adr, char * _data);

功 能: 与 rf_check_write () 函数类似，但使用的是16进制数。

参 数:

icdev: rf_init()返回的设备描述符

Snr: 卡片系列号

Authmode: 密码验证模式

Adr: 块地址

_data: 检查的内容

返 回: = 0: 成功

<>0: 失败

例: unsigned char data[32]="00112233445566778899aabbccddeeff";
unsigned char authmode=0;
st=rf_write_hex(icdev,4,data);
st=rf_check_writehex(icdev,authmode,4,data);

(23) int rf_HL_initval(HANDLE icdev,unsigned char _Mode,unsigned char _SecNr,unsigned long _Value,unsigned long *_Snr);

功 能: 高级初始化值（只用于扇区不用于块）

参 数:

icdev: rf_init()返回的设备描述符

Mode: 高级函数有三种模式

0——IDLE 模式 ，一次只操作一张卡

1——ALL 模式 ，一次可操作多张卡

2——选择模式 ，只操作选中的卡片

_SecNr: 扇区号（0～15）

_Value: 初始化的值

_Snr: 卡片系列号（只在模式2，选择模式中使用）

返 回: = 0: 成功

<>0: 失败

函数操作流程: request（ALL 或 IDLE）

anticoll（SEL=0）

select

authentication

write（DATA）

write（BACKUP）

read （DATA）
read （BACKUP）
compare
halt

例: unsigned long snr;
st=rf_HL_initval(icdev,0x0,3,100L,&snr);

(24) int rf_HL_decrement(HANDLE icdev,unsigned char _Mode,unsigned char _SecNr,unsigned long _Value,unsigned long _Snr,unsigned long *_NValue,unsigned long *_NSnr);

功 能: 高级减值操作（用于扇区）

参 数:

icdev: rf_init()返回的设备描述符
_NValue：将要减去的值
其余参数参见 rf_hl_initval () 函数.

返 回: = 0: 成功
<>0: 失败

函数操作流程: request（ALL 或 IDLE）
anticoll（SEL=0）
select
authentication
read（DATA）
read（BACKUP）
compare
decrement（DATA）
transfer（BACKUP）
restore（BACKUP）
transfer（DATA）
halt

例: unsigned long Snr,Nvalue,NSnr;
st=rf_HL_decrement(icdev,0,2,1,Snr,&Nvalue,&NSnr);

(25) int rf_HL_increment(HANDLE icdev,unsigned char _Mode,unsigned char _SecNr,unsigned long _Value,unsigned long _Snr,unsigned long *_NValue,unsigned long *_NSnr);

功 能: 高级增值操作(用于扇区)

参 数:

_Nvalue: rf_init()返回的设备描述符
其余参数参见 rf_hl_initval () 函数.

返 回: =0: 成功
<>0: 失败

函数操作流程: request（ALL 或 IDLE）
anticoll（SEL=0）
select
authentication

read（DATA）
read（BACKUP）
compare
increment（DATA）
transfer（BACKUP）
restore（BACKUP）
transfer（DATA）
halt

例： unsigned char Snr,Nvalue,NSnr;
st=rf_HL_increment(icdev,0,2,1,Snr,&Nvalue,&NSnr);

(26) int rf_HL_write(HANDLE icdev,unsigned char _Mode,unsigned char _Adr,unsigned long *_Snr,unsigned char *_Data);

功 能: 高级写函数，向选定的并通过密码验证的卡片写入1块16个字节。

参 数:

icdev: rf_init()返回的设备描述符
_Mode: 寻卡模式，与 rf_HL_initval () 函数相似
_Adr: 块地址
_Snr: 卡片系列号（仅用于模式2）
_Data: 写入卡片的数据 (长度为16 字节)

返 回: =0: 成功
<>0: 失败

函数操作流程: request（ALL 或 IDLE）
anticoll（SEL=0）
select
authentication
write（_Adr）
read（_Adr）
halt

例： unsigned long Snr;
unsigned char data[16]="f1f2f3f4f5f6f7f8";
st=rf_HL_write(icdev,0,3,&Snr,data);

(27) int rf_HL_writehex(HANDLE icdev,unsigned char _Mode,unsigned char _Adr,unsigned long *_Snr, char *_Data);

功 能: 16进制高级写操作。

返 回: = 0: 成功
<>0: 失败

例: unsigned char data[32]="f1f2f3f4f5f6f7f8f1f2f3f4f5f6f7f8";
unsigned long Snr;
st=rf_HL_writehex(icdev,0,3,&Snr,data);

(28) int rf_HL_read(HANDLE icdev,unsigned char _Mode,unsigned char _Adr,unsigned long _Snr,unsigned char *_Data,unsigned long *_NSnr);

功 能: 高级读函数，从选定的并通过密码验证的卡片读出1块16个字节。

参 数:

icdev: rf_init()返回的设备描述符

_Mode: 寻卡模式，与 rf_HL_initval ()函数相似

_Adr: 块地址

_Snr: 卡片系列号（仅用于模式2）

_Data: 从卡片中读出的数据 (长度为16 字节)

_NSnr: 返回卡片系列号

返 回: = 0: 成功

<>0: 失败

函数操作流程: request（ALL 或 IDLE）

anticoll（SEL=0）

select

authentication

read（_Adr）

read (BACKUP)

compare

halt

例:

```
unsigned long Snr,NSnr;
unsigned char data[16];
st=rf_HL_read(icdev,0,3,Snr,data,&NSnr);
```

(29) int rf_HL_readhex(HANDLE icdev,unsigned char _Mode,unsigned char _Adr,unsigned long _Snr, char *_Data,unsigned long *_NSnr);

功 能: 高级16进制读操作

返 回: = 0: 成功

<>0: 失败

例:

```
unsigned char data[32];
unsigned long Snr,NSnr;
st=rf_HL_readhex(icdev,0,3,Snr,data,&NSnr);
```

(30) int rf_HL_authentication(HANDLE icdev,unsigned char reqmode, unsigned long snr,unsigned char authmode,unsigned char secnr);

功 能: 高级验证函数(组合了 rf_card() 和 rf_authentication() 函数)

参 数:

icdev: rf_init()返回的设备描述符

reqmode: 寻卡模式，与 rf_HL_initval ()函数相似

snr: 卡片系列号（仅用于模式2）

authmode: 密码验证模式

0 —用 A 密码验证

4 —用 B 密码验证

secnr: 扇区号（0～15）

返 回: =0: 成功

<>0 失败

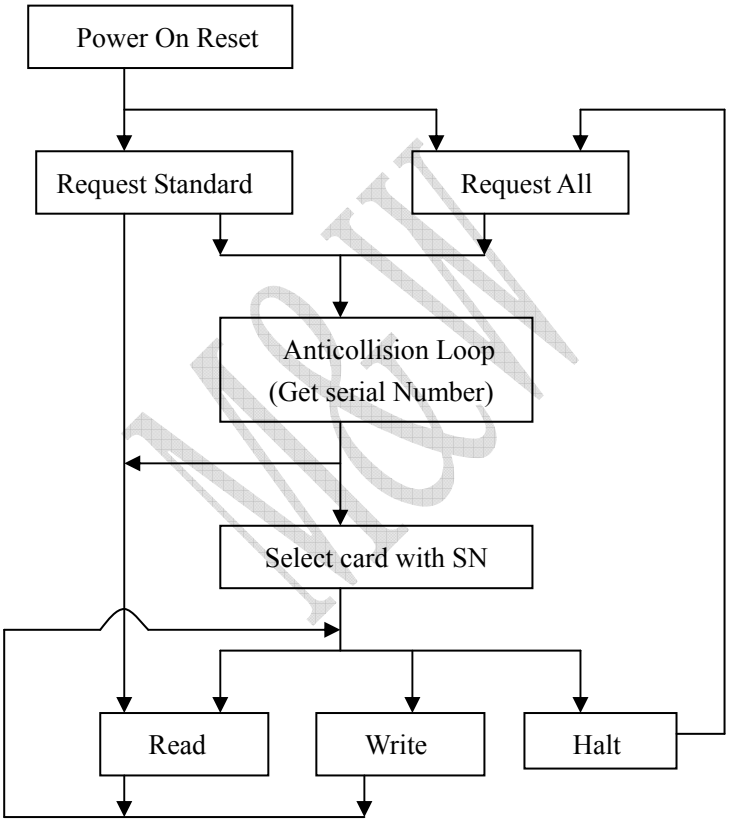
例:

```
unsigned long snr;
st=rf_HL_authentication(icdev,0,snr,0,3);
```

7.4 Mifare UltraLight

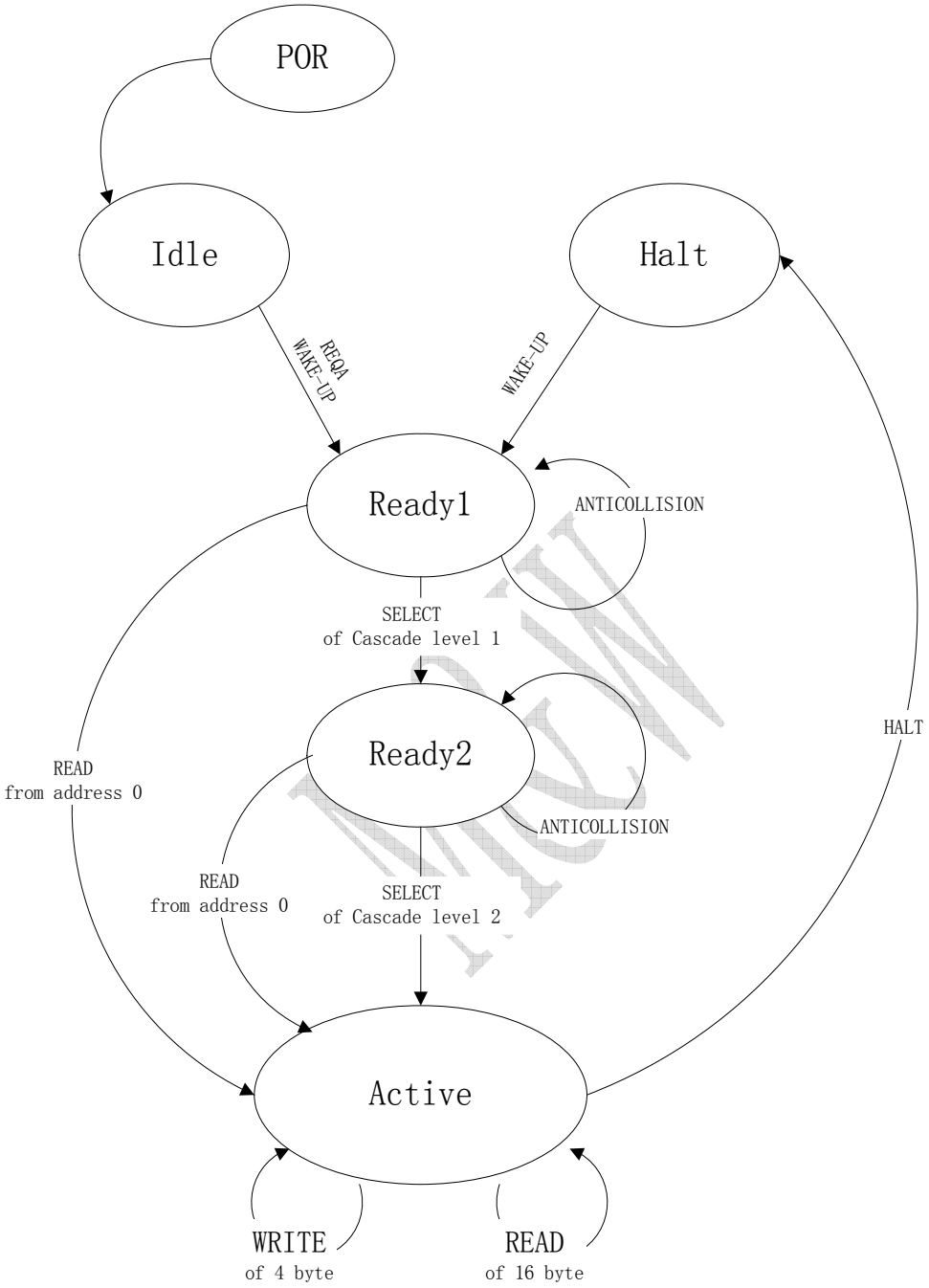
这里只说明了 Mifare UltraLight 卡的操作函数，有关 Mifare UltraLight 卡的资料请参考附录。

7.4.1 操作流程图



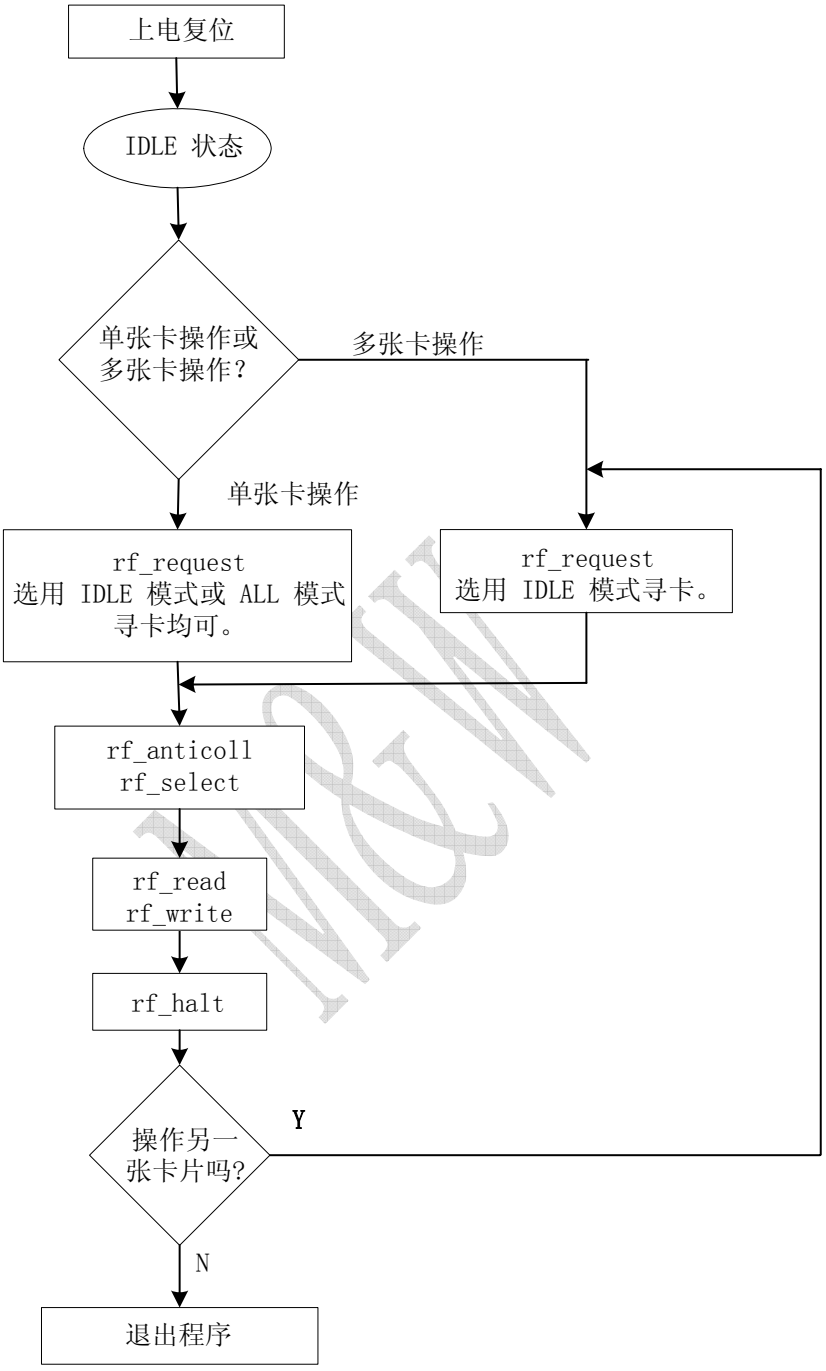
SN: serial number

7.4.2 Mifare UltraLight 状态图



Note:Not shown in this diagram: In each state the command interpreter returns to the Idle state if an unexpected command is received.If the IC has already been in the Halt state vefore it returns to the Halt state in such a case.

7.4.3 函数说明



调用 Mifare UltraLight 卡片 API函数流程图

1) int rf_request(HANDLE icdev,unsigned char _Mode,unsigned __int16 *TagType);

功 能：寻卡请求

参 数：icdev：rf_init()返回的设备描述符

_Mode：U寻卡模式

0 IDLE mode, 只有处在 IDLE 状态的卡片才响应读写器的命令。

1 ALL mode, 处在 IDLE 状态和 HALT 状态的卡片都将响应读写器的命令。

Tagtype：卡类型值，(Mifare std. 1k: 0x0004, UltraLight: 0x0044, FM005: 0x0005, Mifare std. 4k: 0x0002, SHC1122: 0x3300)

返回值: = 0: 成功

<>0: 失败

例：
```
#define IDLE 0x00
int st;
unsigned int *tagtype;
st=rf_request(icdev,IDLE,tagtype);
```

2) int rf_anticoll(HANDLE icdev,unsigned char _Bcnt,unsigned long *_Snr);

功 能：激活读写器的防冲突队列。如果有几张 MIFARE 卡片在感应区内，将会选择一张卡片，并返回卡片的序列号供将来调用 rf_select 函数时使用。

参 数：icdev：rf_init()返回的设备描述符

_Bcnt： 设为 0

_Snr：返回的卡序列号地址

返 回：成功则返回 0

例：
```
int st;
unsigned long snr;
st=rf_anticoll(icdev,0,&snr);
```

注：request 指令之后应立即调用 anticoll，除非卡的序列号已知。

3) int rf_select(HANDLE icdev,unsigned long _Snr,unsigned char *_Size);

功 能：从多个卡中选取一个给定序列号的卡

参 数：icdev：rf_init()返回的设备描述符

_Snr：卡序列号

_Size：指向返回的卡容量的数据

返 回：成功则返回 0

例：
```
int st;
unsigned long snr=239474;
unsigned char size;
st=rf_select(icdev,snr,&size);
```

4) int rf_get_snr(HANDLE icdev,unsigned char *_Snr);

功 能：取 UltraLight 卡片序列号，此种卡的序列号长度为 7 字节

参 数：icdev：rf_init()返回的设备描述符

_Snr： 返回的卡片系列号

_Snr[0] 卡片序列号第 0 字节

. .

. .

_Snr[6] 卡片序列号第 6 字节

返回值: =0: 成功

<>0: 失败

例: int st;

unsigned char _Snr[8];

st = rf_get_snr(icdev, _Snr);

5) int rf_read(HANDLE icdev,unsigned char _Adr,unsigned char *_Data);

功 能：读取卡中数据,一次读一页的数据 ；

参 数:

icdev：rf_init()返回的设备描述符

_Adr: 页地址(0～15)

_Data: 读取的数据

返回值: = 0: 成功

<>0: 失败

例: int st;

unsigned char data[17]；

st=rf_read(icdev,1,data);

6) int rf_read_hex(HANDLE icdev,unsigned char _Adr, char *_Data);

功 能:与 rf_read（）相同，读出的数据以十六进制形式表示

参数:

icdev：rf_init()返回的设备描述符

_Adr: 页地址(0～15)

_Data: 读取的数据，以十六进制形式表示

返回值: =0: 成功

<>0: 失败

例: int st;

unsigned char data[32];

//读页 1 的数据

st=rf_read_hex(icdev,1,data);

7) int rf_write(HANDLE icdev,unsigned char _Adr,unsigned char *_Data);

功 能：向卡中写入一个长度为 16 字节的数据，但是只有低 4 位的字节写入到指定的地址空间中，建议 4-15 字节设为“0”。

参 数：

icdev：rf_init()返回的设备描述符

_Adr： 页地址 ；

_Data：要写入的数据，长度为 16 字节，一页的长度为 4 字节，剩下的 12 个字节初始化为“0”；

返回值: =0: 成功

<>0: 失败

例: int st;

```
unsigned char data[17];
memet(data, 0, 17);
memcpy(data, “\x11\x22\x33\x44”);
st=rf_write(icdev,2,data);          //写第二页
```

8) int rf_write_hex(HANDLE icdev,unsigned char _Adr,char *_Data);

功 能: 用十六进制的形式写

参 数:

icdev：rf_init()返回的设备描述符

_Adr： 页地址 ；

_Data: 写入的数据,长度为 32 字节. 剩下的 24 个字节初始化为“0”;

返回值: =0: 成功

<>0: 失败

例:

```
int st;
unsigned char data[33];
memset(data, 0, 33);
memcpy(data,"a1a2a3a4”,8);
st=rf_write_hex(icdev,1,data);          //写第 1 页
```

9) int rf_halt(HANDLE icdev);

功 能：中止对该卡操作，执行这个指令后，在重新复位之前，不能再对卡进行通讯，除非 rf_request（）的寻卡模式为 ALL。

参 数：

icdev：rf_init()返回的设备描述符

返回值: =0: 成功

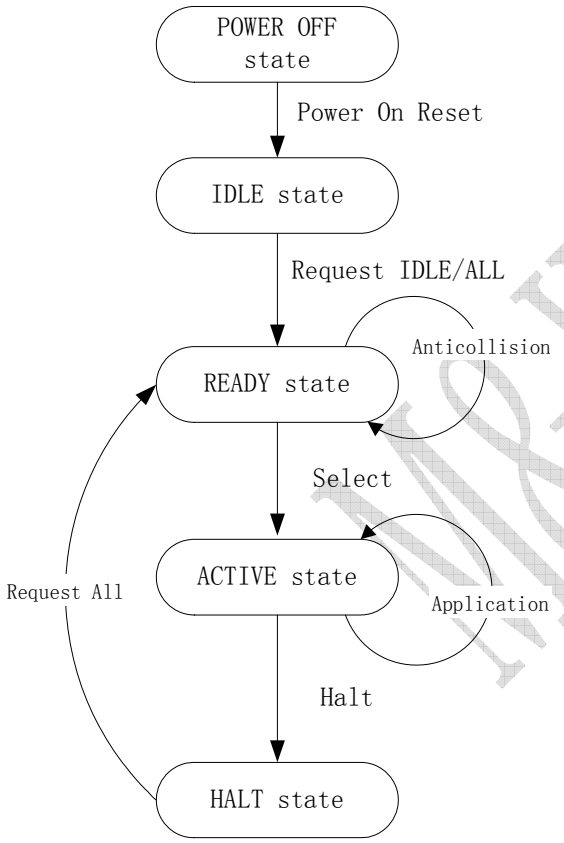
<>0: 失败

例: st=rf_halt(icdev);

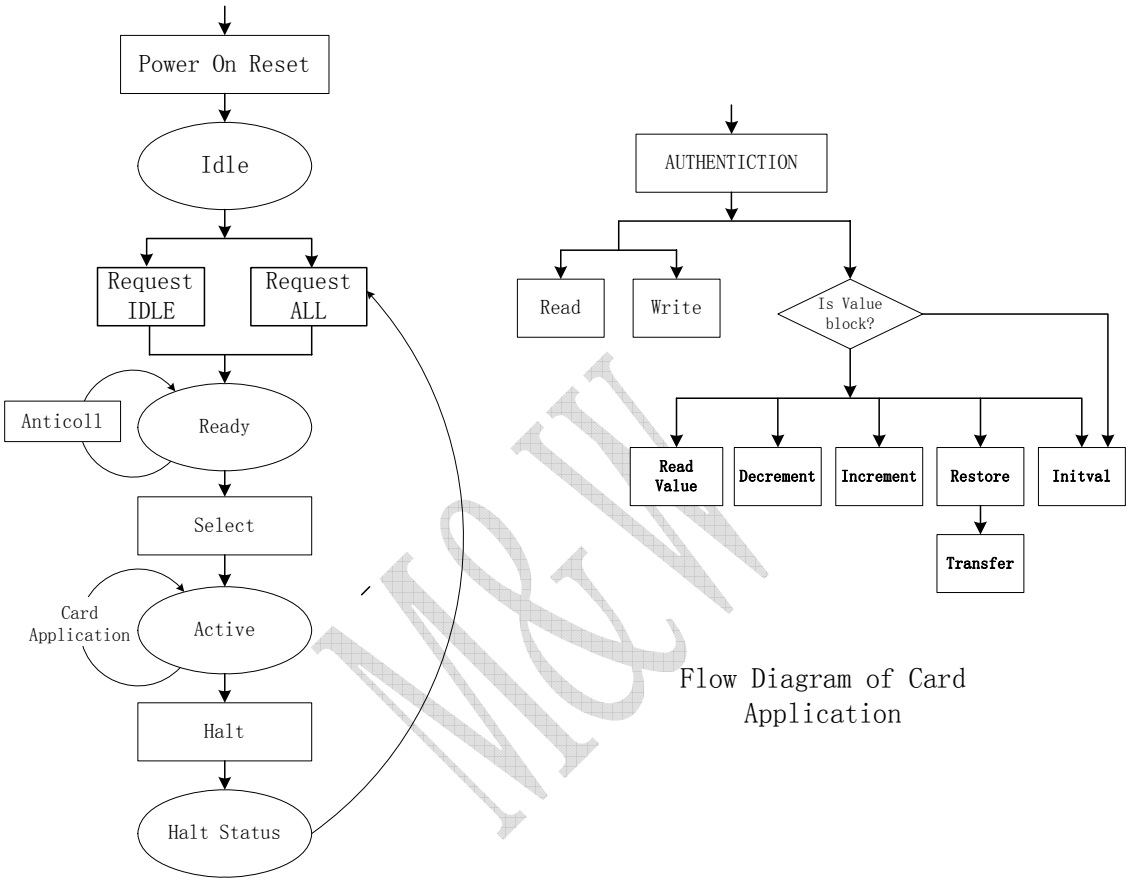
7.5 Mifare Standard 4K

这里只说明了 Mifare Standard 4K 卡的操作函数，有关 Mifare Standard 4K 卡的资料请参考附录。

7.5.1 状态图和指令流程

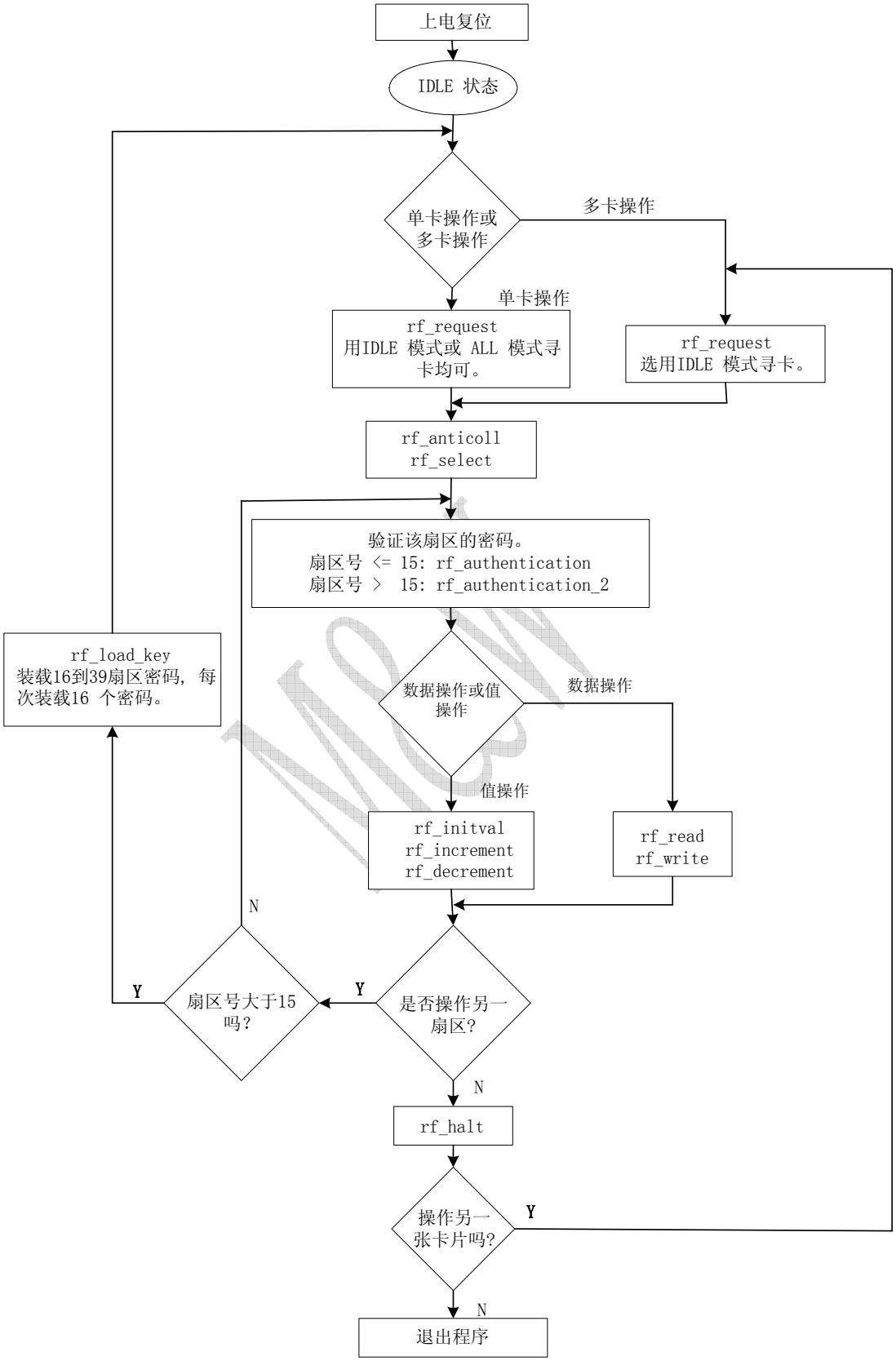


7.5.2 操作流程图



Flow Diagram of Card Application

7.5.3 函数说明:



调用 Mifare std 4K 卡片 API函数流程图

在 mifare 系列卡的操作函数中，针对同一个操作有高级函数和低级函数之分。

7.5.3.1 低级函数

1) int rf_request(HANDLE icdev,unsigned char _Mode,unsigned __int16 *TagType);

功 能：寻卡请求

参 数：icdev：rf_init()返回的设备描述符

_Mode：U 寻卡模式

0 IDLE mode, 只有处在 IDLE 状态的卡片才响应读写器的命令。

1 ALL mode, 处在 IDLE 状态和 HALT 状态的卡片都将响应读写器的命令。

Tagtype：卡类型值，(Mifare std. 1k: 0x0004, UltraLight: 0x0044, FM005: 0x0005, Mifare std. 4k: 0x0002, SHC1122: 0x3300)

返回值: = 0: 成功

<>0: 失败

例：
```
#define IDLE 0x00
int st;
unsigned int *tagtype;
st=rf_request(icdev,IDLE,tagtype);
```

注意：关于寻卡模式指令 ：

如果选择 IDLE 模式寻卡对卡进行读写操作，执行 Urf_halt()Urf_halt 指令中止卡操作后，只有当该卡离开并再次进入操作区时，读写器才能够再次寻到这张卡。

如果选择 ALL 模式寻卡对卡进行操作,执行 Urf_halt()U 命令中止卡操作后,卡可以不必离开操作区.读写器下次也能寻到那张相同的卡.

2) int rf_anticoll(HANDLE icdev,unsigned char _Bcnt,unsigned long *_Snr);

功 能：激活读写器的防冲突队列。如果有几张 MIFARE 卡片在感应区内，将会选择一张卡片，并返回卡片的序列号供将来调用 rf_select 函数时使用。

参 数：

icdev：rf_init()返回的设备描述符

_Bcnt： 设为 0

_Snr：返回的卡序列号地址

返 回：成功则返回 0

例：
```
int st;
unsigned long snr;
st=rf_anticoll(icdev,0,&snr);
```

注：request 指令之后应立即调用 anticoll，除非卡的序列号已知。

3) int rf_select(HANDLE icdev,unsigned long _Snr,unsigned char *_Size);

功 能：从多个卡中选取一个给定序列号的卡，返回卡的容量

参 数：

icdev：rf_init()返回的设备描述符

_Snr：卡序列号
_Size：指向返回的卡容量的数据
返 回：成功则返回 0
例: int st;
unsigned long snr=239474;
unsigned char size;
st=rf_select(icdev,snr,&size);

4) int rf_authentication(HANDLE icdev,unsigned char _Mode,unsigned char _SecNr);

功 能：验证某一扇区密码
参 数：icdev：rf_init()返回的设备描述符
_Mode：密码验证模式
0 — 用 A 密码验证
4 — 用 B 密码验证 mode_auth
_ SecNr：要验证密码的扇区号（0～15）
返 回：成功则返回 0
例： int st;
st=rf_authentication(icdev,0,5); //认证第 5 扇区的密码 A

注：HRF-35LT 系列的读写器只能装载 16 个扇区的密码。16-39 扇区必须调用 rf_authentication_2()验证。

5) int rf_authentication_2(HANDLE icdev,unsigned char _Mode,unsigned char KeyNr,unsigned char Adr);

功 能:用 0—15 扇区的密码来验证指定的扇区
参 数:
icdev：rf_init()返回的设备描述符
_Mode: 验证模式 ， 与 rf_authentication 相同
KeyNr: 密码扇区号 (0~15)
Adr: 要验证的扇区地址 (0~39).
返回值: = 0: 成功
<>0: 失败
例: int st; // 用第 0 单元的密码认证第 0 扇区的密码 A
st=rf_authentication_2(icdev,0,0,0);

6) int rf_authentication_key(HANDLE icdev, unsigned char _Mode, unsigned char _BlockNr, unsigned char *_Key);

功能: 利用函数参数中提供的密码对卡片指定数据块进行认证。如果参数中提供的密码与卡片的密码匹配，则认证成功，反之则认证失败。
参数:
icdev: rf_init()返回的设备描述符
_Mode: 验证密码类型：
0 — 用 KEY A 验证
4 — 用 KEY B 验证
BlockNr: 卡片数据块地址(0~63)
_Key: 用于卡片认证的密码

返回: = 0: 正确
<>0: 错误
例: unsigned char key[] = {0xff, 0xff, 0xff, 0xff, 0xff, 0xff};
st=rf_authentication_key(icdev, 0, 0, key);

7) int rf_read(HANDLE icdev,unsigned char _Adr,unsigned char *_Data);

功 能：读取卡中数据,一次读一个块的数据，为 16 个字节；
参 数：
icdev：rf_init()返回的设备描述符
_Adr：块地址（0~255）；
_Data：读出数据
返 回：成功则返回 0
例： int st;
unsigned char data[17];
st=rf_read(icdev,4,data); //读 M1 卡块 4 的数据

8) int rf_read_hex(HANDLE icdev,unsigned char _Adr, char *_Data);

功 能: 以十六进制形式读取数据；
参 数:
icdev：rf_init()返回的设备描述符
_Adr： 块地址（0～255）；
_Data：读出数据
返回值: =0: 成功
<>0: 失败
例: int st;
unsigned char data[33];
st=rf_read_hex(icdev,1,data); //读取块 1 的数据

9) int rf_write(HANDLE icdev,unsigned char Adr,unsigned char *Data);

功 能：向卡中写入数据,一次必须写一个块，为 16 个字节；
参 数：
icdev：rf_init()返回的设备描述符
_Adr：M1 卡——块地址（1～255）；
_Data：要写入的数据，长度为 16 字节
返回值: =0: 成功
<>0: 失败
例: int st;
unsigned char data[16]={0x00,0x11,0x22,0x33,0x44,0x55,0x66,0x77,
0x88,0x88,0x77,0x66,0x55,0x44,0x33,0x22,0x11};
st=rf_write(icdev,1,data); //写块 1

10) int rf_write_hex(HANDLE icdev,unsigned char _Adr,char *_Data);

功 能: 用十六形式进写
参 数:
icdev：rf_init()返回的设备描述符
_Adr: 块地址(1~255)

_Data: 要写入的数据 ,长度是 32

返回值: =0: 成功

<>0: 失败

例: int st;

unsigned char data[32]="a1a2a3a4a5a6a7a8a1a2a3a4a5a6a7a8";

st=rf_write_hex(icdev,1,data); //写块 1

11) int rf_initval(HANDLE icdev,unsigned char _Adr,unsigned long _Value);

功 能：初始化块值

参 数：

icdev：rf_init()返回的设备描述符

_Adr：块地址

_Value：初始值

返 回：成功则返回 0

例： int st;

unsigned long value=1000;

st=rf_initval(icdev,1,value); /*将块 1 的值初始化为 1000*/

注：在进行值操作时，必须先执行初始化值函数，然后才可以读、减、加的操作.

12) int rf_increment(HANDLE icdev,unsigned char _Adr,unsigned long _Value);

功 能：块加值

参 数：icdev：rf_init()返回的设备描述符

_Adr：块地址

_Value：要增加的值

返 回：成功则返回 0;

例： int st;

unsigned long value=10;

st = rf_increment(icdev, 1, value);

13) int rf_decrement(HANDLE icdev,unsigned char _Adr,unsigned long _Value);

功 能：块减值

参 数：

icdev：rf_init()返回的设备描述符

_Adr：块地址

_Value：要减的值

返 回：成功则返回 0

例： int st;

unsigned long value=10;

st=rf_decrement(icdev,1,value);

14) int rf_readval(HANDLE icdev,unsigned char _Adr,unsigned long *_Value);

功 能：读块值

参 数：

icdev：rf_init()返回的设备描述符

_Adr：块地址

_Value：读出值的地址

返 回：成功则返回 0

例： int st;

unsigned long value;

st=rf_readval(icdev,1,&value); /*读出块 1 的值，放入 value*/

15) int rf_restore(HANDLE icdev,unsigned char _Adr);

功 能：回传函数，将 EEPROM 中的内容传入卡的内部寄存器

参 数：

icdev：rf_init()返回的设备描述符

_Adr：要进行回传的块地址

返 回：成功返回 0

例： int st;

st=rf_restore(icdev,1);

注：用此函数将某一块中的数值传入内部寄存器，然后用 rf_transfer()函数将寄存器中数据再传送到另一块中去，实现块与块之间数值传送。该函数只用于值块。

16) int transfer(HANDLE icdev,unsigned char _Adr);

功 能：传送，将寄存器的内容传送到 EEPROM 中，在 rf_restore（）后执行.

参 数：

icdev：rf_init()返回的设备描述符

_Adr：要传送的地址

返 回：成功返回 0

例： rf_restore(icdev,1);

rf_transfer(icdev,2);

上两行实现将块 1 的内容传送到块 2。

17) int rf_halt(HANDLE icdev);

功 能：中止对该卡操作

参 数：

icdev：rf_init()返回的设备描述符

返 回：成功则返回 0

例：st=rf_halt(icdev);

说明：执行该命令后如果是 ALL 寻卡模式则必须重新寻卡才能够对该卡操作，如果是 IDLE 模式则必须把卡移开感应区再进来才能寻得这张卡。

7.5.3.2 高级函数

18) int rf_card(HANDLE icdev,unsigned char _Mode,unsigned long *_Snr);

功 能：寻卡并返回卡片的系列号，它可以完成低级函数 rf_request, rf_anticoll 和 rf_select 的功能。

参 数：icdev：rf_init()返回的设备描述符

_Mode：U 寻卡模式

0: IDLE 模式

1: ALL 模式

mode_card_Snr：返回的卡序列号

返 回：成功则返回 0

例： int st;

unsigned long snr;

st=rf_card(icdev,0,&snr);IDLE 模式寻卡

注意：rf_card() 由三个低级函数组成 :rf_request(),rf_select() and rf_anticoll()。

如果选择 IDLE 模式寻卡对卡进行读写操作，执行 Urf_halt()Urf_halt 指令中止卡操作后，只有当该卡离开并再次进入操作区时，读写器才能够再次寻到这张卡。

如果选择 ALL 模式寻卡对卡进行操作,执行 Urf_halt()U 命令中止卡操作后,卡可不必离开操作区.读写器下次也能寻到那张相同的卡

19) int rf_changeb3(HANDLE icdev,unsigned char _SecNr,unsigned char *_KeyA,unsigned char _B0,unsigned char _B1,unsigned char _B2,unsigned char _B3,unsigned char _Bk,unsigned char *_KeyB);

功 能：修改块 3 的数据

参 数：icdev：rf_init()返回的设备描述符

_SecNr：扇区号

_KeyA：密码 A

_B0：块 0 控制字，低 3 位（D2D1D0）对应 C10、C20、C30

_B1：块 1 控制字，低 3 位（D2D1D0）对应 C11、C21、C31

_B2：块 2 控制字，低 3 位（D2D1D0）对应 C12、C22、C32

_B3：块 3 控制字，低 3 位（D2D1D0）对应 C13、C23、C33

_Bk：保留参数，取值为 0

_KeyB：密码 B

返 回：成功则返回 0

例： int st;

unsigned char keya[6]={0xa0,0xa1,0xa2,0xa3,0xa4,0xa5};

unsigned char keyb[6]={0xb0,0xb1,0xb2,0xb3,0xb4,0xb5};

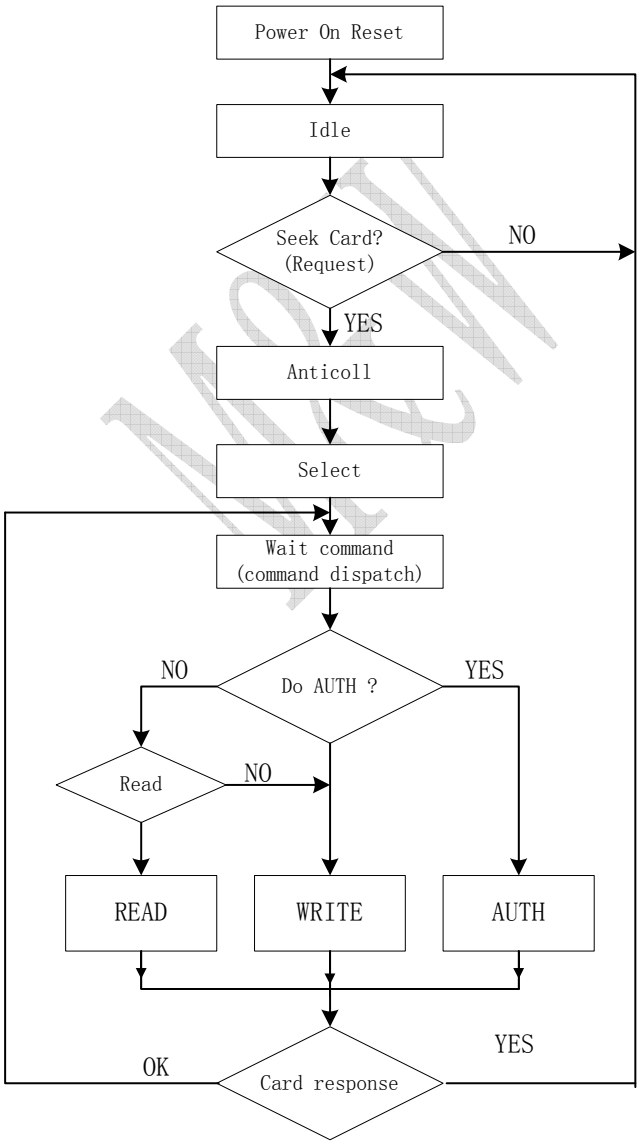
st=rf_changeb3(icdev,keya,0x04,0x04,0x04,0x04,0,keyb);

8 复旦筹码卡操作函数

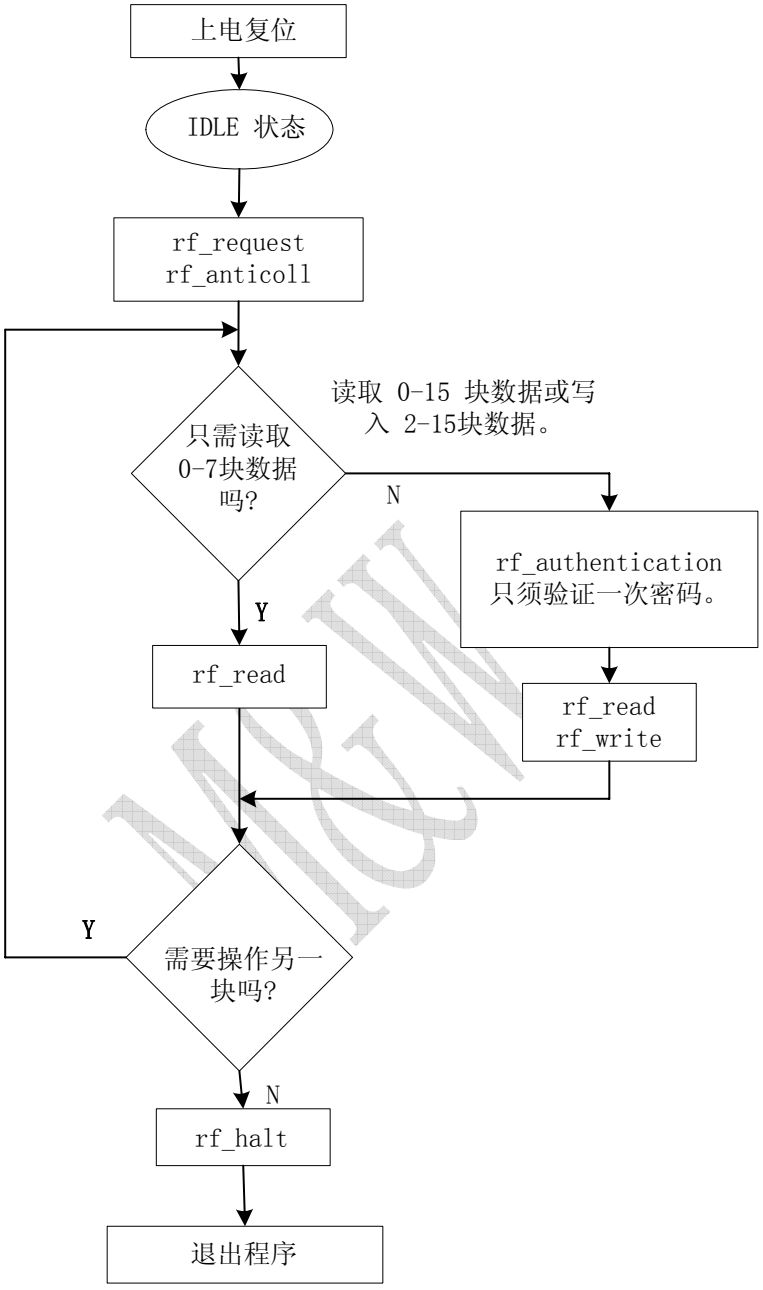
8.1 复旦非接触卡 FM11RF005

这里只说明了复旦 FM11RF005 卡的操作函数，有关 复旦 FM11RF005 卡的资料请参考附录。

8.1.1 FM11RF005 操作流程



8.1.2 函数说明：



调用 FUDAN FM005 卡片 API函数流程图

1) 选卡

int rf_request(HANDLE icdev,unsigned char _Mode,unsigned __int16 *TagType)

功 能：寻卡请求

参 数：icdev：rf_init()返回的设备描述符

_Mode：U 寻卡模式

0 IDLE 模式 一次对一张卡操作

1 ALL 模式 一次可对多张卡操作.mode_card

Tagtype：卡类型值，(Mifare std. 1k: 0x0004, UltraLight: 0x0044, FM005: 0x0005, Mifare std. 4k: 0x0002, SHC1122: 0x3300)

返回值: = 0: 成功

<>0: 失败

例：
```
#define IDLE 0x00
int st;
unsigned int *tagtype;
st=rf_request(icdev,IDLE,tagtype);
```

int rf_anticoll(HANDLE icdev,unsigned char _Bcnt,unsigned long *_Snr);

功 能：卡防冲突，返回卡的序列号

参 数：icdev：rf_init()返回的设备描述符

_Bcnt： 设为 0

_Snr：返回的卡序列号地址

返 回：成功则返回 0

例：
```
int st;
unsigned long snr;
st=rf_anticoll(icdev,0,&snr);
```

注：request 指令之后应立即调用 anticoll，除非卡的序列号已知。

int rf_select(HANDLE icdev,unsigned long _Snr,unsigned char *_Size);

功 能：从多个卡中选取一个给定序列号的卡，返回卡的容量

参 数：icdev：rf_init()返回的设备描述符

_Snr：卡序列号

_Size：指向返回的卡容量的数据

返 回：成功则返回 0

例：
```
int st,type;
unsigned char size;
unsigned long snr;
rf_request(icdev,0,&type);
rf_anticoll(icdev,0,&snr);
st=rf_select(icdev,snr,&size);
```

int rf_card(HANDLE icdev,unsigned char _Mode,unsigned long *_Snr);

功 能:寻卡并返回卡的序列号

参 数: icdev：rf_init()返回的设备描述符

_Mode: 寻卡模式

0: IDLE 模式

1: ALL 模式

_Snr: 返回卡的序列号

返 回 =0 : 成功

<>0 : 失败

例: int st;

unsigned char Mode=0; //IDLE mode

unsigned long snr;

st=rf_card(icdev,Mode,&snr);

注意：rf_card() 由三个低级函数构成:rf_request(), rf_select() and rf_anticoll()。

2) 验证密码

对于需要认证的卡片，这里有两种认证方式：装载密码认证和直接密码认证。

➢ **装载密码认证**

优点：

- 安全性高

  装载密码认证是指将密码下载到读写器存储单元，PC 机发送卡片认证指令后读写器从存储单元取出相应的密码进行卡片认证。由于密码下载到读写器存储单元后是不可读的，并且下载到读写器的密码在读写器断电后不会丢失，所以可以在安全的地方将密码下载到读写器，减少了密码在通讯过程中的传输次数。
- 装载密码可以和卡片交易分开，可以在不同的时间和地点进行。

缺点：

读写器密码存储单元有使用寿命，一般为十万次，如果装载过于频繁超过使用寿命，它将会坏掉不能再装载密码。

int rf_load_key(HANDLE icdev,unsigned char _Mode,unsigned char _SecNr,unsigned char *_NKey);

功 能: 将密码装入读写模块 RAM 中，没有数据交换。

在读写器中有 16 个扇区的空间，但是 FM005 只有一个密码，用于密码验证的块号必须与装载密码的扇区号相同

参 数: icdev：rf_init()返回的设备描述符

_Mode: 0

_SecNr: 装载密码的扇区号（0-15）

_Nkey: 写入读写器的 6 字节密码, 因为 FM005 只要 4 个字节的密码, 所以后 2 位可以设为 0。

返回: = 0: 成功

<>0: 失败

例 : unsigned char key[6]= {0xa0,0xa1,0xa2,0xa3,0xa4,0xa5 }

st=rf_load_key(icdev,0,1,key);//在扇区 1 中装载第 0 套 A 密码

int rf_load_key_hex(HANDLE icdev,unsigned char _Mode,unsigned char _SecNr,char *_NKey);

功 能: 与 rf_load_key 相似, 用十六进制表示

参 数 : icdev：rf_init()返回的设备描述符

Mode: 0

_SecNr: 装载密码的扇区号（0-15）

_Nkey: 写入读写器的 12 字节密码, 因为 FM005 只要 4 个字节的密码, 所以后 4

位可以设为 0。

返 回: =0: 成功

<>0: 失败

例: / load the 0PthP key A “a0a1a2a3a4a5” into sector 1

char key[]= “a0a1a2a3a4a5”;

st=rf_load_key_hex(icdev,0,1,key);

int rf_authentication(HANDLE icdev,unsigned char _Mode,unsigned char _SecNr);

功 能: .用读写器中的密码与所访问卡的密码进行验证，如果读写器的密码与卡中的密码一致，则验证通过。

参 数: icdev：rf_init()返回的设备描述符

_Mode: 0

_SecNr: 要访问的卡扇区号（0-15）

返回: = 0: 成功

<>0: 失败

例： int st;

//authentication the 5th sector whit the 0PthP key A

st=rf_authentication(icdev,0,5);//用第 0 套 A 密码验证第 5 个扇区

注意: 因为 FM005 只有一个密码，所以用于密码验证的块号要与装载密码的扇区号相同

- **直接密码认证**

优点：方便，没有使用寿命限制。

直接密码认证是指 PC 机向读写器发送卡片认证指令时将认证密码作为命令参数一起发送，直接使用参数中的密码对卡片进行认证。

缺点：安全性不够

由于每次对卡片认证时，密码都会在通讯过程中传输，所以密码的安全性必须由应用商自己保证，通过其他方式来保证密码的安全性。

int rf_authentication_key(HANDLE icdev, unsigned char _Mode, unsigned char _BlockNr, unsigned char *_Key);

功能: 利用函数参数中提供的密码对卡片指定数据块进行认证。如果参数中提供的密码与卡片的密码匹配，则认证成功，反之则认证失败。

参数:

icdev: rf_init()返回的设备描述符

_Mode: 验证密码类型：

0 — 用 KEY A 验证

4 — 用 KEY B 验证

BlockNr: 卡片数据块地址(0~15)

_Key: 用于卡片认证的密码

返回: = 0: 正确

<>0: 错误

例: unsigned char key[] = {0xff, 0xff, 0xff, 0xff, 0xff, 0xff};

st=rf_authentication_key(icdev, 0, 0, key);

3) 读一个数据块

int rf_read(HANDLE icdev,unsigned char _Adr,unsigned char *_Data);

功 能: .从一个已选择的卡中读取一个数据块

参 数:

icdev：rf_init()返回的设备描述符

_Adr: 要读取的数据块（0-15）

_Data: 读出的数据.

返 回: = 0: 成功

<>0: 失败 r

例: int st;

unsigned char data[16]；

st=rf_read(icdev,1,data);

int rf_read_hex(HANDLE icdev,unsigned char _Adr, char *_Data);

功 能: 读一个数据块，十六进制表示数据

参 数:

icdev：rf_init()返回的设备描述符

_Adr: 要读取的数据块（ 0~15）

Data:读出的数据， 与 rf_read()相同.

返回: =0: 成功

<>0: 失败

例 : int st;

unsigned char data[32];

st=rf_read_hex(icdev,1,data); //读块 1 的数据

4) 写一个数据块

int rf_write(HANDLE icdev,unsigned char _Adr,unsigned char *_Data);

功 能：向卡中写入数据 ，一次必须写一个块，为 16 个字节；

参 数：

icdev：rf_init()返回的设备描述符

_Adr：要写数据的块地址（2-15）；

_Data：要写入的数据

返 回：成功则返回 0

例： int st;

unsigned char *data={0x00,0x11,0x22,0x33,0x44,0x55,0x66,0x77,

0x88,0x88,0x77,0x66,0x55,0x44,0x33,0x22,0x11};

st=rf_write(icdev,4,data);//写第四块

int rf_write_hex(HANDLE icdev,unsigned char _Adr,char *_Data);

功 能：以十六进制形式写

参 数：

icdev：rf_init()返回的设备描述符

_Adr：要写数据的块地址（2-15）；

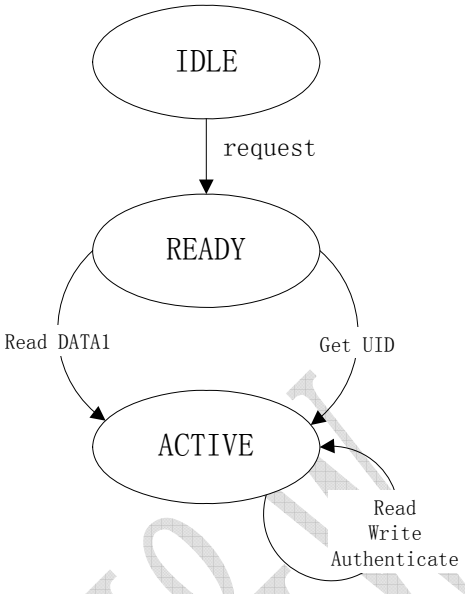
_Data：要写入的数据

返回: =0: 成功
<>0: 失败
例: int st;
unsigned char data[32]="a1a2a3a4a5a6a7a8a1a2a3a4a5a6a7a8";
st=rf_write_hex(icdev,1,data);

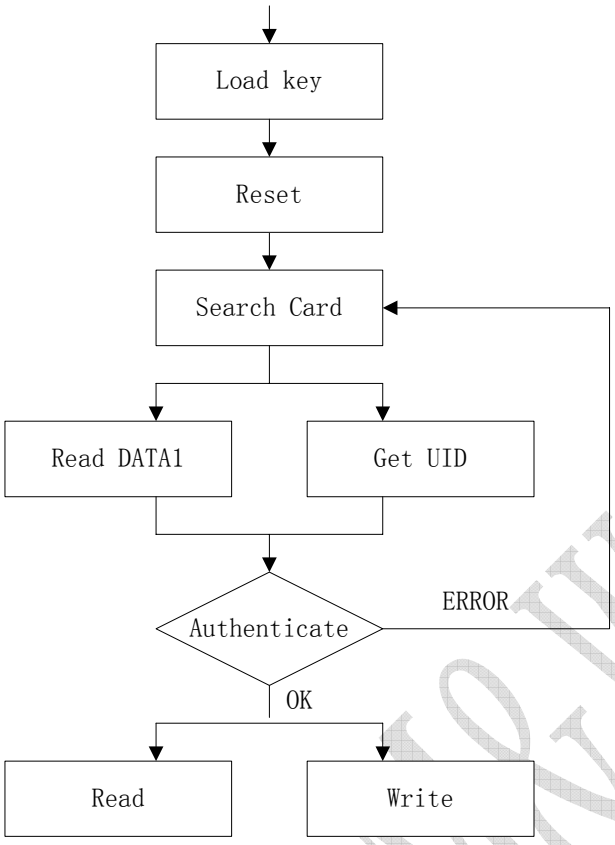
5) HALT:
中止对卡操作，如果想继续对卡操作，需要重新寻卡。
int rf_halt(HANDLE icdev);
功 能: 中止对卡操作，如果想继续对卡操作，需要重新寻卡。
参数:
icdev：rf_init()返回的设备描述符
返 回: =0: 成功
<>0: 失败
例: st=rf_halt(icdev);

9 华虹 SHC1102 卡操作函数

9.1 状态图



9.2 SHC1102 操作流程



注意：

1) 可以在认证密码前的任何时候装载密码到读写器，但密码必须装载到读写器的第八个密码单元。
2) 当卡片放到读写器天线范围内，必须先调用 rf_reset()函数对射频复位，然后才能寻卡等卡片操作。
3) 当卡片操作失败时，如果还需要对卡片操作，必须冲新寻卡。

9.3 函数说明

1) 选卡

int rf_request(HANDLE icdev,unsigned char _Mode,unsigned __int16 *TagType)

功 能：寻卡请求

参 数：icdev：rf_init()返回的设备描述符

_Mode：U 寻卡模式

0 IDLE 模式 一次对一张卡操作

1 ALL 模式 一次可对多张卡操作

Tagtype：卡类型值，(Mifare std. 1k: 0x0004, UltraLight: 0x0044, FM005: 0x0005, Mifare std. 4k: 0x0002, SHC1122: 0x3300)

返回值: = 0: 成功

<>0: 失败

例：
```
#define IDLE 0x00
int st;
unsigned int *tagtype;
st=rf_request(icdev,IDLE,tagtype);
```

int rf_anticoll(HANDLE icdev,unsigned char _Bcnt,unsigned long *_Snr);

功 能：卡防冲突，返回卡的序列号

参 数：icdev：rf_init()返回的设备描述符

_Bcnt： 设为 0

_Snr：返回的卡序列号地址

返 回：成功则返回 0

例：
```
int st;
unsigned long snr;
st=rf_anticoll(icdev,0,&snr);
```

注：request 指令之后应立即调用 anticoll，除非卡的序列号已知。

int rf_select(HANDLE icdev,unsigned long _Snr,unsigned char *_Size);

功 能：从多个卡中选取一个给定序列号的卡，返回卡的容量

参 数：icdev：rf_init()返回的设备描述符

_Snr：卡序列号

_Size：指向返回的卡容量的数据

返 回：成功则返回 0

例：
```
int st,type;
unsigned char size;
nsigned long snr;
rf_request(icdev,0,&type);
rf_anticoll(icdev,0,&snr);
  st=rf_select(icdev,snr,&size);
```

int rf_card(HANDLE icdev,unsigned char _Mode,unsigned long *_Snr);

功 能:寻卡并返回卡的序列号

参 数:

icdev：rf_init()返回的设备描述符

_Mode: 寻卡模式

0: IDLE 模式

1: ALL 模式

_Snr: 返回卡的序列号

返 回 =0 : 成功

<>0 : 失败

例: int st;

unsigned char Mode=0; //IDLE mode

unsigned long snr;

st=rf_card(icdev,Mode,&snr);

注意：rf_card() 由三个低级函数构成:rf_request(), rf_select() and rf_anticoll()。

2) 验证密码

对于需要认证的卡片，这里有两种认证方式：装载密码认证和直接密码认证。

➢ **装载密码认证**

优点：

- 安全性高

  装载密码认证是指将密码下载到读写器存储单元，PC 机发送卡片认证指令后读写器从存储单元取出相应的密码进行卡片认证。由于密码下载到读写器存储单元后是不可读的，并且下载到读写器的密码在读写器断电后不会丢失，所以可以在安全的地方将密码下载到读写器，减少了密码在通讯过程中的传输次数。

- 装载密码可以和卡片交易分开，可以在不同的时间和地点进行。

缺点：

读写器密码存储单元有使用寿命，一般为十万次，如果装载过于频繁超过使用寿命，它将会坏掉不能再装载密码。

int rf_load_key(HANDLE icdev,unsigned char _Mode,unsigned char _SecNr,unsigned char *_NKey);

功 能: 将密码装入读写模块 RAM 中，没有数据交换。

在读写器中有 16 个扇区的空间，但是 SHC11002 只有一个密码，用于密码验证的块号必须与装载密码的扇区号相同且必须为 8.

参 数:

icdev：rf_init()返回的设备描述符

_Mode: 0

_SecNr: 装载密码的扇区号，必须为 8

_Nkey: 写入读写器的 6 字节密码, 因为 SHC1102 只要 4 个字节的密码, 所以后 2 位可以设为 0。

返回: = 0: 成功

<>0: 失败

例 : unsigned char key[6]= {0xff,0xff,0xff,0xff,0x00,0x00 }

st=rf_load_key(icdev,0,8,key);

int rf_load_key_hex(HANDLE icdev,unsigned char _Mode,unsigned char _SecNr,char *_NKey);

功 能: 与 rf_load_key 相似, 用十六进制表示

参 数 :

icdev：rf_init()返回的设备描述符

_Mode: 0

_SecNr: 装载密码的扇区号，必须为 8

_Nkey: 写入读写器的 6 字节密码, 因为 SHC1102 只要 4 个字节的密码, 所以后 2 位可以设为 0。

返 回: =0: 成功

<>0: 失败

例: char key[]= “ffffffff0000”;

st=rf_load_key_hex(icdev,0,8,key);

int rf_authentication(HANDLE icdev,unsigned char _Mode,unsigned char _SecNr);

功 能: .用读写器中的密码与所访问卡的密码进行验证，如果读写器的密码与卡中的密码一致，则验证通过。

参 数:

icdev：rf_init()返回的设备描述符

_Mode: 0

_SecNr: 要访问的卡扇区号（0-15）

返回: = 0: 成功

<>0: 失败

例： int st;

st=rf_authentication(icdev,0,8);

注意: 因为 SHC1102 只有一个密码，所以用于密码验证的块号要与装载密码的扇区号相同，且必须为 8.

➢ **直接密码认证**

优点：方便，没有使用寿命限制。

直接密码认证是指 PC 机向读写器发送卡片认证指令时将认证密码作为命令参数一起发送，直接使用参数中的密码对卡片进行认证。

缺点：安全性不够

由于每次对卡片认证时，密码都会在通讯过程中传输，所以密码的安全性必须由应用商自己保证，通过其他方式来保证密码的安全性。

int rf_authentication_key(HANDLE icdev, unsigned char _Mode, unsigned char _BlockNr, unsigned char *_Key);

功能: 利用函数参数中提供的密码对卡片指定数据块进行认证。如果参数中提供的密码与卡片的密码匹配，则认证成功，反之则认证失败。

参数:

icdev: rf_init()返回的设备描述符

_Mode: 验证密码类型：

0 — 用 KEY A 验证

4 — 用 KEY B 验证

BlockNr: 卡片数据块地址(0~15)

_Key: 用于卡片认证的密码
返回: = 0: 正确
<>0: 错误
例: unsigned char key[] = {0xff, 0xff, 0xff, 0xff, 0xff, 0xff};
st=rf_authentication_key(icdev, 0, 8, key);

3) 读一个数据块

int rf_read(HANDLE icdev,unsigned char _Adr,unsigned char *_Data);

功 能: .从一个已选择的卡中读取一个数据块
参 数:
icdev：rf_init()返回的设备描述符
_Adr: 要读取的数据块（0-15）
_Data: 读出的数据，由于 shc1102 卡每个块为 4 字节数据，所以返回的数据是指定地址起始的连续 4 个块的数据。
返 回: = 0: 成功
<>0: 失败 r
例: int st;
unsigned char data[16]；
st=rf_read(icdev,1,data);

int rf_read_hex(HANDLE icdev,unsigned char _Adr, char *_Data);

功 能: 读一个数据块，十六进制表示数据
参 数:
icdev：rf_init()返回的设备描述符
_Adr: 要读取的数据块（ 0~15）
Data:读出的数据， 与 rf_read()相同.
返回: =0: 成功
<>0: 失败
例 : int st;
unsigned char data[32];
st=rf_read_hex(icdev,1,data); //读块 1 的数据

4) 写一个数据块

int rf_write(HANDLE icdev,unsigned char _Adr,unsigned char *_Data);

功 能：向卡中写入一个块的数据；
参 数：icdev：rf_init()返回的设备描述符
_Adr：要写数据的块地址（2-15）；
_Data：要写入的数据，该缓冲区必须大于等于 16，实际写入的数据只有开始的四个字节。
返 回：成功则返回 0
例： int st;
unsigned char data[17];
memset(data, 0, 17);
data[0]=0x11;data[1]=0x22;data[2]=0x33;data[3]=0x44;
st=rf_write(icdev,4,data);//写第四块

int rf_write_hex(HANDLE icdev,unsigned char _Adr,char *_Data);

功 能：向卡中写入一个块的数据。

参 数：icdev：rf_init()返回的设备描述符

_Adr：要写数据的块地址（2-15）；

_Data：要写入的数据，该缓冲区必须大于等于 32， 实际写入的数据只有开始的 8 个字符， 该参数必须为十六进制字符。

返回: =0: 成功

<>0: 失败

例： int st;

char data[33];

memset(data, 0, 33);

strcpy(data, “11223344”);

st=rf_write_hex(icdev,4,data);//写第四块

5) HALT:

中止对卡操作，如果想继续对卡操作，需要重新寻卡。

int rf_halt(HANDLE icdev);

功 能: 中止对卡操作，如果想继续对卡操作，需要重新寻卡。

参数:

icdev：rf_init()返回的设备描述符

返 回: =0: 成功

<>0: 失败

例: st=rf_halt(icdev);

10 SAM/CPU 卡操作函数

10.1 SAM Reset

int rf_sam_rst(HANDLE icdev, unsigned char baud, unsigned char *samack)

功能：SAM 卡复位

参数：

icdev: rf_init()返回的设备描述符

baud: SAM 卡复位波特率

1: 9600 2: 19200 3: 38400 4:76800

samack: SAM 卡复位应答信息

返回： =0: 成功

<>0: 失败

例如： int st = 0;

unsigned char samack[250];

st=rf_sam_rst(icdev, 1, samack); //the baudrate is 9600

10.2 SAM 指令传输

int rf_sam_trn(HANDLE icdev, unsigned char *samblock,unsigned char *recv)

功能：这个函数用来传输 SAM 卡 COS 指令，并返回指令应答信息。

参数：

icdev: rf_init()返回的设备描述符

samblock: SAM 卡 COS 指令信息

samblock[0] NAD(节点地址，可以设置为 0)

samblock[1] pcb(协议控制字节，可以设置为 0)

samblock[2] len(指令信息长度)

samblock[3] SAM 卡指令第 1 字节

. .

. .

samblock[len+3] SAM 卡指令第 len＋3 字节

recv: 返回的 SAM 卡指令应答信息

recv[0] NAD

recv[1] pcb

recv[2] len(应答信息长度)

recv[3] 指令应答信息第 1 字节

. .

. .

recv[len+3] 指令应答信息第 len 字节

返回： =0: 成功

<>0: 失败

例如： int st = 0;
unsigned char sendblock[250], receive[250];
memset(sendblock, 0, 250);
memset(receive, 0, 250);
sendblock[0]=0; sendblock[1]=0; sendblock[2]=5;
memcpy(&sendblock[3], “\x00\x84\x00\x00\x08”, 5); \\ Get challenge
st=rf_sam_trn(icdev, sendblock, receive);

10.3 CPU Reset

int rf_cpu_rst(HANDLE icdev, unsigned char baud, unsigned char *cpuack)
功能：CPU 卡复位
参数：
icdev: rf_init()返回的设备描述符
baud: CPU 卡复位波特率
1: 9600 2: 19200 3: 38400 4:76800
cpuack: CPU 卡复位应答信息
返回： =0: 成功
<>0: 失败
例如： int st = 0;
unsigned char cpuack[250];
st=rf_cpu_rst(icdev, 1, cpuack); //the baudrate is 9600

10.4 CPU 指令传输

int rf_cpu_trn(HANDLE icdev, unsigned char *cpublock,unsigned char *recv)
功能：这个函数用来传输 CPU 卡 COS 指令，并返回指令应答信息。
参数：
icdev: rf_init()返回的设备描述符
cpublock: CPU 卡 COS 指令信息
cpublock[0] NAD(节点地址，可以设置为 0)
cpublock[1] pcb(协议控制字节，可以设置为 0)
cpublock[2] len(指令信息长度)
cpublock[3] CPU 卡指令第 1 字节
. .
. .
cpublock[len+3] SAM 卡指令第 len＋3 字节
recv: 返回的 CPU 卡指令应答信息
recv[0] NAD
recv[1] pcb
recv[2] len(应答信息长度)
recv[3] 指令应答信息第 1 字节
. .

recv[len+3] 指令应答信息第 len 字节

返回： =0: 成功

<>0: 失败

例如： int st = 0;

unsigned char sendblock[250], receive[250];

memset(sendblock, 0, 250);

memset(receive, 0, 250);

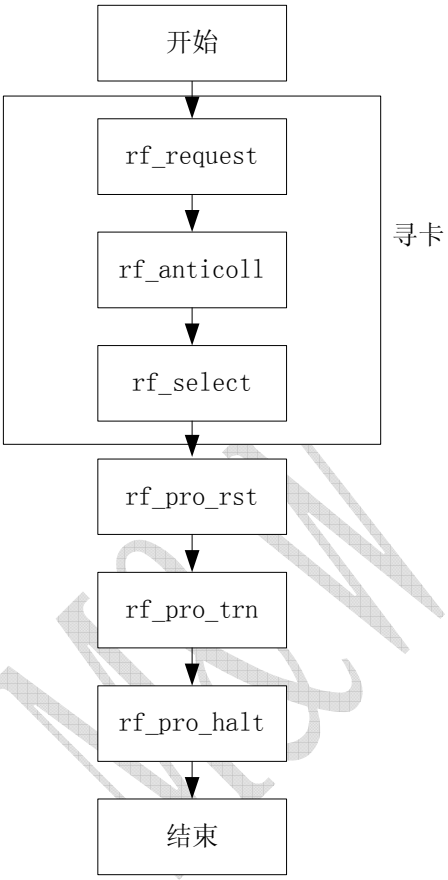
sendblock[0]=0; sendblock[1]=0; sendblock[2]=5;

memcpy(&sendblock[3], “\x00\x84\x00\x00\x08”, 5); \\ Get challenge

st=rf_cpu_trn(icdev, sendblock, receive);

11 MIFAREPRO 卡操作函数

11.1 卡片操作流程



11.2 MIFAREPRO 操作函数

1) int rf_request(HANDLE icdev,unsigned char _Mode,unsigned __int16 *TagType)

功 能: 该函数向卡片发出寻卡命令，开始选择一张新卡片时需要执行该函数。

参 数:

icdev: rf_init()返回的设备描述符

_Mode: 寻卡模式:

0 IDLE mode, 只有处在 IDLE 状态的卡片才响应读写器的命令。

1 ALL mode, 处在 IDLE 状态和 HALT 状态的卡片都将响应读写器的命令。

Tagtype: 返回卡片类型 (Mifare std. 1k: 0x0004, UltraLight: 0x0044, FM005: 0x0005, Mifare std. 4k: 0x0002, SHC1122: 0x3300)

返 回: =0: 成功

<>0: 失败

例如： int st = 0;

unsigned int tagtype;

st=rf_request(icdev, 0, &tagtype);

2) int rf_anticoll(HANDLE icdev,unsigned char _Bcnt,unsigned long *_Snr)

功 能: 激活读写器的防冲突队列。如果有几张 MIFARE 卡片在感应区内，将会选择一张卡片，并返回卡片的序列号供将来调用 rf_select 函数时使用。

参 数:

icdev: rf_init()返回的设备描述符

_Bcnt: 预选卡片使用的位, 标准调用时为 bcnt=0.

_Snr: 返回的卡片序列号

返 回: = 0: 成功

<>0: 失败

例如： int st;

unsigned long snr;

st=rf_anticoll(icdev,0,&snr);

3) int rf_select(HANDLE icdev,unsigned long _Snr,unsigned char *_Size)

功 能: 用指定的序列号选择卡片，将卡片的容量返回给 PC 机。

参 数:

icdev: rf_init()返回的设备描述符

_Snr: 卡片的序列号

_Size: 卡片容量的地址指针，目前该值不能使用

返 回: = 0: 成功

<>0: 失败

例如： int st;

unsigned long snr=239474;

unsigned char size;

st=rf_select(icdev,snr,&size);

4) int rf_pro_rst(HANDLE icdev,unsigned char *_Data)

功能：MIFAREPRO 卡激活

参数：

icdev: rf_init()返回的设备描述符

_Data: MIFAREPRO 卡激活返回的信息

返回： = 0: 成功

<>0: 失败

例如：
```
int st;
unsigned char _Data[256];
memset(_Data,0,256);
st=rf_pro_rst(icdev,_Data);
```

5) int rf_pro_trn(HANDLE icdev,unsigned char *problock,unsigned char *recv)

功能：该函数用于传输 MIFAREPRO 卡 COS 指令，并返回指令应答信息。

参数:

icdev: rf_init()返回的设备描述符

problock: MIFAREPRO 卡指令信息

problock[0]	NAD(节点地址，可以设置为 0)
problock[1]	CID(卡标识符, 可以设置为 0)
problock[2]	PCB(协议控制字节)
problock[3]	len(指令信息长度)
problock[4]	MIFAREPRO 卡指令第 1 字节
.	.
.	.
problock[len+4]	MIFAREPRO 卡指令第 len 字节

recv: MIFAREPRO 卡指令应答信息

recv[0]	NAD
recv[1]	CID
recv[2]	PCB
recv[3]	len(MIFAREPRO 卡指令应答信息长度)
recv[4]	MIFAREPRO 卡指令应答信息第 1 字节
.	.
.	.
recv[len+4]	MIFAREPRO 卡指令应答信息第 len 字节

返回： =0: 成功

<>0: 失败

例如：
```
int st;
unsigned char problock[256];
unsigned char recv[256];
problock[0]=0;
problock[1]=0;
problock[2]=0;
problock[3]=7;
memcpy(&problock[4],"\x80\xe0\x00\x01\x02\x3f\x00",7);
memset(recv,0,256);
st=rf_pro_trn(icdev,problock,recv);
```

6) int rf_pro_halt(HANDLE icdev)

功能：该函数用于解除卡片激活状态，卡片进入 HALT 状态。向卡片传输任何指令，卡片都将不做任何响应，必须重新激活卡片。

参数：

icdev: rf_init()返回的设备描述符

返回： =0: 成功

<>0: 失败

例如： int st;

st=rf_pro_halt(icdev);

附录 非接触卡片的特性

1 MIFARE STANDARD 1K

特性:

- 1K 字节 EEPROM
- 分为16个扇区，每个扇区包括4 块，每块16个字节，以块为存取单位
- 用户可自定义每个存储块的访问条件
- 每张卡有唯一序列号，为32位
- 具有防冲突机制，支持多卡操作
- 非接触传送数据和无源 (卡中无电源)
- 至少10 年数据保存期
- 至少10万次擦写
- 读写距离: 在100mm 内(与天线形状有关)
- 工作频率: 13.56 MHZ
- 通信速率: 106kbit/s
- 典型交易过程: <100 ms(包括备份管理)
- 温度范围: -20℃~50℃

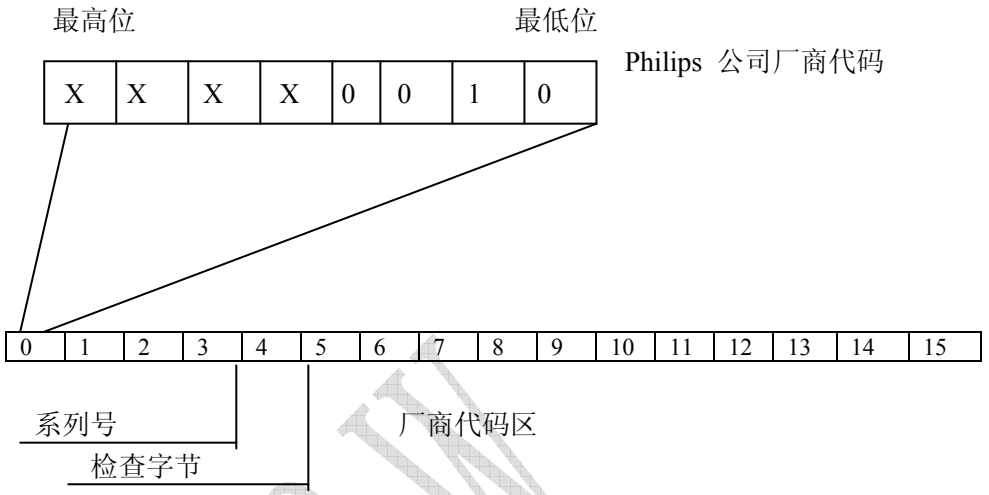
存储结构:

1. 1024*8 位 EEPROM 存储区分为16 个扇区，每扇区分为4块(块0, 块1, 块2, 块3)，按块号编址为0～63共64块。存储区的分布图如下:

扇区号	序号	1 2 3 4 5	6 7 8 9	10 11 12 13 14 15	名称	块号
	0				厂商代码区	0
0	1				数据区	1
	2				数据区	2
	3	A 密码	存取控制	B 密码	扇区 0 控制块区	3
	0				数据区	4
1	1				数据区	5
	2				数据区	6
	3	A 密码	存取控制	B 密码	扇区 1 控制块区	7
			⋮			

	0				数据区	60
15	1				数据区	61
	2				数据区	62
	3	A 密码	存取控制	B 密码	扇区 15 控制块区	63

厂商代码区: 第0扇区的块0（即绝对地址0块）用于存放厂商代码，已经固化，不可更改。



数据区: 所有扇区都有3块（每块16个字节）存储数据。 (扇区0只有两个数据块和一个只读厂商代码块)

值块: 值块可用作电子钱包（有效的命令有：

read,write,increment,decrement,restore,transfer）.每个值块的值为4个字节。

2. 扇区控制块(块 3): 每个扇区都有一个扇区控制块包括：
   - 密码 A 和密码 B(可选), 读取时返回 “0”
   - 访问该扇区4块的存取控制

   如果不需要密码 B，块3的最后6个字节可用作数据。

控制属性

各扇区的块 0、块 1、块 2 为**数据块**，用于存贮数据；块 3 为**控制块**，存放密码 A、存取控制、密码 B，其结构如下：

A0A1A2A3A4A5 FF 07 80 69 B0B1B2B3B4B5

密码 A(6 字节) 存取控制(4 字节) 密码 B(6 字节)

每个扇区的密码和存取控制都是独立的，可以根据实际需要设定各自的密码及存取控制。在**存取控制**中每个块都有相应的三个**控制位**, 定义如下：

块 0： C10 C20 C30
块 1： C11 C21 C31
块 2： C12 C22 C32
块 3： C13 C23 C33

三个控制位以正和反两种形式存在于存取控制字节中，决定了该块的访问权限（如进行减值操作必须验证 KEY A，进行加值操作必须验证 KEY B，等等）。三个控制位在存取控制字节中的位置如下（字节 9 为备用字节，默认值为 0x69）：

	bit 7	6	5	4	3	2	1	0
字节 6	C23_b	C22_b	C21_b	C20_b	C13_b	C12_b	C11_b	C10_b
字节 7	C13	C12	C11	C10	C33_b	C32_b	C31_b	C30_b
字节 8	C33	C32	C31	C30	C23	C22	C21	C20

（注： _b 表示取反）

其中，黑色区控制**块 3**，蓝色区控制**块 2**，绿色区控制**块 1**，红色区控制**块 0**。

数据块（块 0、块 1、块 2）的存取控制如下：

控制位(X=0..2)			访 问 条 件 （对块 0、1、2）			
C1X	C2X	C3X	Read	Write	Increment	Decrement transfer restore
0	0	0	KeyA|B	KeyA|B	KeyA|B	KeyA|B
0	1	0	KeyA|B	Never	Never	Never
1	0	0	KeyA|B	KeyB	Never	Never
1	1	0	KeyA|B	KeyB	KeyB	KeyA|B
0	0	1	KeyA|B	Never	Never	KeyA|B
0	1	1	KeyB	KeyB	Never	Never
1	0	1	KeyB	Never	Never	Never
1	1	1	Never	Never	Never	Never

（KeyA|B 表示密码 A 或密码 B，Never 表示任何条件下不能实现）

例如：当块 0 的存取控制位 C10 C20 C30=100 时，验证密码 A 或密码 B 正确后可读；验证密码 B 正确后可写；不能进行加值、减值操作。

控制块（块 3）的存取控制与**数据块**（块 0、1、2）不同，它的存取控制如下：

控制位			密码 A		存取控制		密码 B	
C13	C23	C33	Read	Write	Read	Write	Read	Write
0	0	0	Never	KeyA|B	KeyA|B	Never	KeyA|B	KeyA|B
0	1	0	Never	Never	KeyA|B	Never	KeyA|B	Never
1	0	0	Never	KeyB	KeyA|B	Never	Never	KeyB
1	1	0	Never	Never	KeyA|B	Never	Never	Never
0	0	1	Never	KeyA|B	KeyA|B	KeyA|B	KeyA|B	KeyA|B

0	1	1	Never	KeyB	KeyA|B	KeyB	Never	KeyB
1	0	1	Never	Never	KeyA|B	KeyB	Never	Never
1	1	1	Never	Never	KeyA|B	Never	Never	Never

例如：当块 3 的存取控制位 C13 C23 C33=100 时，表示：

密码 A： 不可读，验证 KEYB 正确后，可写（更改）。

存取控制：验证 KEYA 或 KEYB 正确后，可读不可写。

密码 B： 不可读，验证 KEYB 正确后，可写。

工作原理

卡片的电气部分只由一个天线和 ASIC 组成。

天线：卡片的天线是只有几组绕线的线圈，很适于封装到 ISO 卡片中。

ASIC:卡片的 ASIC 由一个高速(106KB 波特率)的 RF 接口,一个控制单元和一个 8K 位 EEPROM 组成。

读写器向 M1 卡发一组固定频率的电磁波，卡片内有一个 LC 串联谐振电路，其频率与讯写器发射的频率相同，在电磁波的激励下，LC 谐振电路产生共振，从而使电容内有了电荷，在这个电容的另一端，接有一个单向导通的电子泵，将电容内的电荷送到另一个电容内储存，当所积累的电荷达到 2V 时，此电容可做为电源为其它电路提供工作电压，将卡内数据发射出去或接取读写器的数据。

功能介绍：

1. **Request Standard/ALL:** 一张卡上电复位后就可以响应读写器发出的寻卡命令。读写器向天线范围内的所有卡片发出命令，并识别卡片的型号。
2. **Anticollision Loop:**在防冲突循环中将读出卡片的系列号。如果有几张卡片都在读写器的读写范围内，可以通过唯一的系列号区别它们，并选中其中一张卡片，其余没有选中的卡片将进入等待状态，等待下一次寻卡命令。
3. **Select Card:** 用选卡命令读写器选择一张卡片来进行密码验证和有关的存储操作。卡片将对代码为08h 的选卡命令 ATS 做出响应，该命令决定了所选卡片的类型。
4. **3 Pass Authentication:** 读写器选中一张卡片后就指定了后续存取访问的存储空间，并以次响应开始3重密码验证。
5. **HALT:** 调用 rf_halt () 函数来停止对卡片的所有操作，卡片进入 HALT 状态。
6. **Memory Operations:** 密码验证通过后，可进行以下操作：
   - **读块:** 读取一个存储块的内容
   - **写块:** 写入一个存储块的内容.
   - **减值:** 减少一个块的值并保存在内部寄存器内
   - **增值:** 增加一个块的值并保存在内部寄存器内
   - **保存:** 将块的内容写入数据寄存器中
   - **传输:** 将内部寄存器的内容写入某一块中

   注:用 rf_ restore () 函数将某一块的内容传到内部寄存器内，然后用 rf_truansfer() 函数将内部寄存器的内容传到卡片其余块中。通过这种方法，可以将数据从一块传向另一块。

2 MIFARE UlTRALIGHT

特性:

- 容量为512位，分为16页，每页4个字节
- 每页可编程锁定只读功能
- 32位用户可定义的一次性编程区域
- 384位用户读、写区域
- 唯一的7字节序列号
- 非接触传送数据和无源 (卡中无电源)
- 读写距离：在100mm 以内（与天线有关）
- 工作频率：13.56MHZ
- 通信速率：106KB 波特率
- 完整的数据格式: 16 位 CRC, 奇偶校验,位编码,位计数
- 防冲突：同一时间可处理多张卡
- 数据可保留 2 年
- 可循环改写 1000 次
- 典型交易过程: <35 ms(包括备份管理)
- 快速计数: <10 ms

存储结构:

UltraLight 卡共 512 位，分为 16 页，每页为 4 个字节。存储结构如下：

页号	字节 0	字节 1	字节 2	字节 3	说明
0	SN0	SN1	SN2	BCC0	Serial Number
1	SN3	SN4	SN5	SN6	Serial Number
2	BCC1	保留	Lock0	Lock1	保留/Lock
3	OTP0	OTP1	OTP2	OTP3	OTP
4	Data0	Data1	Data2	Data3	Data read/write
5	Data4	Data5	Data6	Data7	Data read/write
6	Data8	Data9	Data10	Data11	Data read/write
7	Data12	Data13	Data14	Data15	Data read/write
8	Data16	Data17	Data18	Data19	Data read/write
9	Data20	Data21	Data22	Data23	Data read/write
10	Data24	Data25	Data26	Data27	Data read/write
11	Data28	Data29	Data30	Data31	Data read/write
12	Data32	Data33	Data34	Data35	Data read/write
13	Data36	Data37	Data38	Data39	Data read/write
14	Data40	Data41	Data42	Data43	Data read/write

15	Data44	Data45	Data46	Data47	Data read/write

（1） 第 0、1 页存放着卡的序列号等信息，只可读。依据 ISO/IEC14443-3 校验位计算如下：

BCC0=CT ⊕ SN0 ⊕ SN1 ⊕ SN2

BCC1=SN3 ⊕ SN4 ⊕ SN5 ⊕ SN6

（2） 第 2 页为 LOCK BYTES，设置字节 2 和字节 3 对应的位可以将从第 3 页到 15 页单独地锁定为只读区域。

Lock0

L 7	L 6	L 5	L 4	L OTP	BL 15-10	BL 9-4	BL OTP

Lock1

L 15	L 14	L 13	L 12	L 11	L 10	L 9	L 8

Lx 锁定 X 页为只读

BLX 锁定对应的 Lx 位

注意：一旦 block-locking(BLX)位被设置为锁定配置，对应的内存区域将被冻结。如：BL15-10 设置为 1，则 L15 到 L10 再也不能改变。Lock0 和 Lock1 可以通过写命令来设置，写入的内容与当前内容进行位或操作得到新的内容，初始值为 0。该过程是不可逆转的。如果有一个位被置为 1，就再也不能置为 0。

（3） 第 3 页为 OTP，即一次性编程，初始值为 0。可以通过写命令来改变它的值，写入的值和当前值进行位或操作得到新的值。这个过程是不可逆转的。如果一个位被置为 1，将再也不能置回 0。

注意：该内存区域可以用作最大值为 32 的一次性计数器。

（4） 第 4 到 15 页为用户读/写区域，初始值为 0。

函数说明：

UltraLight 卡是一种单程票非接触式 IC 卡。

1、 卡片指令

reset--->request--->anticoll--->select--->read、write--->halt

2、 函数特别说明

UltraLight 卡操作函数同 Mifare One，有以下几点需要说明：

- 由于 UltraLight 卡的序列号为 7 个字节，所以防冲突函数不能够返回全部的卡片序列号，如要取得全部的卡片序列号请调用 rf_get_snr 函数，该函数为 UltraLight 卡专用函数。
- UltraLight 卡没有密码，故不需要装载密码，也不存在认证指令。
- Rf_read 函数返回 16 个字节的数据（即 4 个 page），故用户给的缓冲区必须大于 16 个字节。
- Rf_write 函数写入 16 个字节的数据，实际只有前面 4 个字节的数据写入指定的地址，其余字节可以补零。
- UltraLight 卡不存在增值、减值指令。
- 不支持高级函数。

功能介绍:

1. REQA/Wake-Up: 将卡片放入读写范围内,使它进入 ready 状态。Mifare Light 在 Idle 状态只接受 REQA 命令，在 Idle 和 Halt 状态.只接受 WAKE-UP 命令。

2. ANTICOLLISION AND SELECT: 这两个命令用在防冲突循环中。防冲突命令获取系列号部分，选卡命令用这个系列号从读写范围中的多张卡片中选择一张卡片。

3. **READ:** 根据页地址读出 16 个字节的内容。可以循环读取数据，例：如果页地址是 14，那么将读出 14，15，0，1 页的内容。

4. **WRITE:** 写卡命令用来对 2 页的锁字节，3 页的 OTP 字节，4 页到 15 页的数据字节进行操作。一个写卡命令完成一页的操作是指对一行共 4 个字节的操作。

5. **HALT:** 暂停命令用来将已操作完的卡设置进入等待状态（以 Halt 状态代替了 Idle 状态），这样就可以把已进行过防冲突处理，已知 UID 的卡片简单区别开来。这种机制是使读写器能在读写区域寻找到所有卡片的一个很有效的方法。

3 MIFARE STANDARD 4K

特性:

- 容量为4K 字节 EEPROM, 分为40个扇区，其中32个扇区为4个块，8个扇区为16个块，每块16个字节,以块为存取单位
- 每个扇区有独立的一组密码及访问控制
- 三重密码验证
- 每张卡有唯一序列号，为32位
- 具有防冲突机制，支持多卡操作
- 工作频率：13.56MHZ
- 完整的数据格式: 16 位 CRC, 奇偶校验,位编码,位计数
- 典型交易过程: <100 ms(包括备份管理)
- 非接触传送数据和无源 (卡中无电源)
- 读写距离：在100mm 以内（与天线有关）
- 数据可保留10年
- 可循环改写100,000次

存储结构：

Mifare 4KByte 卡分为 40 个扇区，第 0 到 31 扇区每个扇区 4 块（块 0～3），第 32 到 39 扇区每个扇区 16 块，共 256 个块。按块号编址为 0～255。第 0 扇区的块 0（即绝对地址 0 块）用于存放厂商代码，已经固化，不可更改。前 32 个扇区的块 0、块 1、块 2 为**数据块**，用于存贮数据；块 3 为**控制块**，存放密码 A、存取控制、密码 B。后 8 个扇区的块 0 到块 14 为数据块，块 15 为控制块。控制块的结构如下：

A0A1A2A3A4A5	FF 07 80 69	B0B1B2B3B4B5
密码 A(6 字节)	存取控制(4 字节)	密码 B(6 字节)

控制属性

每个扇区的密码和存取控制都是独立的，可以根据实际需要设定各自的密码及存取控制。在**存取控制**中每个块都有相应的三个**控制位**,定义如下：

块 0：	C10	C20	C30
块 1：	C11	C21	C31
块 2：	C12	C22	C32
块 3：	C13	C23	C33

三个控制位以正和反两种形式存在于存取控制字节中，决定了该块的访问权限（如进行减值操作必须验证 KEY A，进行加值操作必须验证 KEY B，等等）。三个控制位在存取控制字节中的位置如下（字节 9 为备用字节，默认值为 0x69）：

	bit 7	6	5	4	3	2	1	0
字节 6	C23_b	C22_b	C21_b	C20_b	C13_b	C12_b	C11_b	C10_b
字节 7	C13	C12	C11	C10	C33_b	C32_b	C31_b	C30_b
字节 8	C33	C32	C31	C30	C23	C22	C21	C20

（注： _b 表示取反）

其中，黑色区控制**块 3**，蓝色区控制**块 2**，绿色区控制**块 1**，红色区控制**块 0**。

数据块（块 0、块 1、块 2）的存取控制如下：

控制位(X=0..2)			访 问 条 件 （对块 0、1、2）			
C1X	C2X	C3X	Read	Write	Increment	Decrement transfer restore
0	0	0	KeyA|B	KeyA|B	KeyA|B	KeyA|B
0	1	0	KeyA|B	Never	Never	Never
1	0	0	KeyA|B	KeyB	Never	Never
1	1	0	KeyA|B	KeyB	KeyB	KeyA|B
0	0	1	KeyA|B	Never	Never	KeyA|B
0	1	1	KeyB	KeyB	Never	Never
1	0	1	KeyB	Never	Never	Never
1	1	1	Never	Never	Never	Never

（KeyA|B 表示密码 A 或密码 B，Never 表示任何条件下不能实现）

例如：当块 0 的存取控制位 C10 C20 C30=100 时，验证密码 A 或密码 B 正确后可读；验证密码 B 正确后可写；不能进行加值、减值操作。

控制块（块 3）的存取控制与**数据块**（块 0、1、2）不同，它的存取控制如下：

控制位			密码A		存取控制		密码B	
C13	C23	C33	Read	Write	Read	Write	Read	Write
0	0	0	Never	KeyA|B	KeyA|B	Never	KeyA|B	KeyA|B
0	1	0	Never	Never	KeyA|B	Never	KeyA|B	Never
1	0	0	Never	KeyB	KeyA|B	Never	Never	KeyB
1	1	0	Never	Never	KeyA|B	Never	Never	Never
0	0	1	Never	KeyA|B	KeyA|B	KeyA|B	KeyA|B	KeyA|B
0	1	1	Never	KeyB	KeyA|B	KeyB	Never	KeyB
1	0	1	Never	Never	KeyA|B	KeyB	Never	Never

1	1	1	Never	Never	KeyA|B	Never	Never	Never

例如：当块 3 的存取控制位 C13 C23 C33=100 时，表示：

密码 A： 不可读，验证 KEYB 正确后，可写（更改）。

存取控制：验证 KEYA 或 KEYB 正确后，可读不可写。

密码 B： 不可读，验证 KEYB 正确后，可写。

工作原理

卡片的电气部分只由一个天线和 ASIC 组成。

天线：卡片的天线是只有几组绕线的线圈，很适于封装到 ISO 卡片中。

ASIC：卡片的 ASIC 由一个高速（106KB 波特率）的 RF 接口，一个控制单元和一个 8K 位 EEPROM 组成。

读写器向 M1 卡发一组固定频率的电磁波，卡片内有一个 LC 串联谐振电路，其频率与讯写器发射的频率相同，在电磁波的激励下，LC 谐振电路产生共振，从而使电容内有了电荷，在这个电容的另一端，接有一个单向导通的电子泵，将电容内的电荷送到另一个电容内储存，当所积累的电荷达到 2V 时，此电容可做为电源为其它电路提供工作电压，将卡内数据发射出去或接取读写器的数据。

注意事项：

1) 对于装载密码认证方式，由于明华公司 HRF-35LT 读写器只能保存一套 16 个扇区的密码，所以扇区号大于 15 扇区的密码必须重新装载，同时调用认证函数 rf_authentication_2( )。

例如：

```
int   sector=16,mode=0;
HANDLE icdev;
Unsigned data[17];
rf_authentication_2(icdev, mode, sector%16, sector*4);
rf_read(icdev, sector*4, data);
```

2) 值操作中数据块的长度为 4 字节，存储结构如下：

字节号	0 1 2 3	4 5 6 7	8 9 10 11	12	13	14	15
描述	Value	Value_b	Value	Addr	Addr_b	Addr	Addr_b

注（_b：表示取反）

功能介绍：

1. **Request Standard/ALL**: 一张卡上电复位后就可以响应读写器发出的寻卡命令。读写器向天线范围内的所有卡片发出命令，并识别卡片的型号。
2. **Anticollision Loop :**在防冲突循环中将读出卡片的系列号。如果有几张卡片都在读写器的读写范围内，可以通过唯一的系列号区别它们，并选中其中一张卡片，其余没有选中的卡片将进入等待状态，等待下一次寻卡命令。
3. **Select Card:** 用选卡命令读写器选择一张卡片来进行密码验证和有关的存储操作。卡片将对代码为 08h 的选卡命令 ATS 做出响应，该命令决定了所选卡片的类型。

4. **Pass Authentication:** 读写器选中一张卡片后就指定了后续存取访问的存储空间，并以次响应开始 3 重密码验证。

5. **HALT:** 调用 rf_halt () 函数来停止对卡片的所有操作，卡片进入 HALT 状态。

6. **Memory Operations:** 密码验证通过后，可进行以下操作：
   - 读块: 读取一个存储块的内容
   - 写块: 写入一个存储块的内容.
   - 减值:减少一个块的值并保存在内部寄存器内
   - 增值: 增加一个块的值并保存在内部寄存器内
   - 保存: 将块的内容写入数据寄存器中
   - 传输: 将内部寄存器的内容写入某一块中

   注:用 rf_ restore () 函数将某一块的内容传到内部寄存器内，然后用 rf_truansfer() 函数将内部寄存器的内容传到卡片其余块中。通过这种方法，可以将数据从一块传向另一块。

4 复旦 FM11RF005

特性:

- 512 位的 EEPROM 存储单元
- 半双工通讯方式
- 每张卡有唯一的序列号
- 无防冲突机制
- 工作频率：13.56MHz
- 通讯波特率：106kbit/s
- 操作距离：≤ 6 cm
- 可支持 Mifare 或上海地方三重防伪认证标准
- 至少 10 年数据保存期
- 温度范围：－20℃～＋50℃
- 至少 100,000 次擦写循环

存储结构：

卡片的通用存储器分 3 个区、16 个 Block，每个 Block 包括 4 个字节。存储结构如表 1 所示。

块号	说明
0	筹码标识(2 字节客户代码、2 字节厂商代码)
1	筹码序列号（4 字节）
2	数据块
3	数据块
4	数据块
5	数据块
6	数据块
7	数据块
8	密码块（4 字节）
9	数据块
10	数据块
11	数据块
12	数据块
13	数据块
14	数据块
15	数据块

表 1

卡片的读写权限如表 2 所示。

Block Number	未认证	认证后
0~1	只可读	只可读
2~7	只可读	可读/可写
8~15	不可读/不可写	可读/可写

表 2

卡片说明：

FUDAN FM005 卡兼容上海市地方标准《城市轨道交通单程票非接触式集成电路（IC）卡》，适用于城市轨道交通单程票和各类计费和数据采集系统的应用。

1、**卡片指令**

i. reset--->request--->anticoll --->read--->halt

ii. ---> authertication--->read、write--->halt

2、**特别说明**

1) 由于筹码型卡只有一个密码，所以只需要对其中任意一个块认证通过后，即可对其它的块进行读写操作。
2) 装载密码时，由于筹码型卡的密码为 4 字节，所以后面两个字节必须补 0。
3) 选中卡片后，如果执行认证、读操作和写操作的其中任一操作失败，则必须对卡片重新寻卡。
4) 筹码型卡无防冲突功能，调用该函数只是为了返回卡片序列号。如果同时有两张或两张以上卡片，则防冲突失败，不会有序列号返回。
5) 筹码型卡每个块只有 4 个字节。rf_write 函数，写入 16 字节的数据，实际只有 4 个字节的数据写入到指定地址，其余的数据可以补 0。Rf_read 函数返回 16 字节的数据，即指定地址开始的 4 个块的数据。
6) 筹码型卡不存在增值和减值命令，所以增值和减值功能必须由写指令来实现。
7) 不支持高级函数。

功能介绍：

FM005 卡片已用做城市轨道交通系统的单程票。它是一种非接触集成电路筹码卡，支持 REQALL/REQA, READ, WRITE 和 AUTH 命令。

1. **Request Standard/ALL:** 读写器向读写范围内的卡片发出寻卡命令，并区分卡片的类型。
2. **READ:**从卡片上读出一块的内容。
3. **WRITE:** 向卡片写入一块的内容。
4. **AUTH:** 读写器和卡片之间的三重密码认证。

5 华虹 shc1102

特性:

- 工作频率：13.56 MHz
- 通信速率：106 kbit/s
- 调制方式：ISO/IEC 14443 Type A
- 工作温度：-20℃至 80℃
- 存贮容量：512 bits
- 无电池： 无线方式传递数据和能量
- 读写距离：在距读卡器天线 0-100 mm 区域内能正确进行数据交换和完成各项操作
- 采用半双工通讯协议
- 在无线通讯过程中通过以下机制来保证数据完整

---每帧有16位 CRC 检验
---每字节有奇偶校验位

- 数据安全性

---相互认证
---每张卡的序列号惟一
---传输密钥保护

- 灵活的的存储结构

---512 位 EEPROM （16 Blocks × 4 Bytes × 8 Bits ）
---分为2个不同访问条件的数据区 （ DATA 1、DATA 2 ）
---每个块为最小访问单位，由4个字节组成
---每个芯片可定义自己独立的密钥 （4 Bytes ）

- 数据保持时间大于 10 年
- 擦写次数大于 10 万次

交易流程:

当华虹 SHC1102 位于读写器的有效工作范围之外时，芯片处于无电状态，不能进行任何操作；当其进入读写器的有效工作范围，芯片上电复位，进入等待状态，在此状态下可正确接收和响应读写器发送的询卡/应答指令，并进行相互认证和读写等操作。

- 询卡(Answer to Request)

读写器通过发出指令来确认是否有华虹非接触式 IC 卡产品（SHC1101、SHC1102）进入其操作范围，并通过应答确认产品的类型。并由产品类型确定相互之间的通讯协议和

通讯速率。

- 选卡（Select）

  选择要进入下一步操作的卡序列号（UID），卡应在确认被选中后返回卡的用户码（CID）。

- 认证(Authentication)

  SHC1102 进入读写器的有效工作范围并正确响应之后，读写器与 SHC1102 电子标签之间要进行相互认证。只有都通过了认证，读写器才能开始对卡进行权限操作（非权限读操作无需认证即可进行）。

- 读写(Read/Write)

  在完成必要的认证后,读写器就可以开始对 SHC1102 进行读写操作了。

  读——读一个块，直接读或经认证后读。

  写——写一个块，必须先通过认证。

- 停止（Halt）

  将 SHC1102 设置为停止等待状态。

存储结构及其读写权限

SHC1102 中的 EEPROM 存储区容量为 512 Bits，分成 16 个块，每个块由 4 个字节组成，每个字节有 8 位。块是存储区的最小访问单位。

SHC1102 芯片中 EEPROM 存储区的结构如表 1 所示。

表 1 SHC1102 芯片中存储结构表

Block No.	Byte 1	Byte 2	Byte 3	Byte 4
0	CID0	CID1	MID0	MID1
1	UID0	UID1	UID2	UID3
2	DATA 1	DATA 1	DATA 1	DATA 1
… …	DATA 1	DATA 1	DATA 1	DATA 1
7	DATA 1	DATA 1	DATA 1	DATA 1
8	Password	Password	Password	Password
9	DATA 2	DATA 2	DATA 2	DATA 2
… …	DATA 2	DATA 2	DATA 2	DATA 2
15	DATA 2	DATA 2	DATA 2	DATA 2

●制造商块

块 0、块 1 是特殊的数据块，用于存放制造商代码（MID）、客户代码（CID）、唯一序列号（UID），称制造商块。制造商块中的数据由芯片制造商在生产过程中写入，数据只读，不可改写。

●密钥块

块 8 专用于存放认证的密钥，称密钥块，此块存放的数据须通过认证后才可读或可改写。

●应用数据区 1 （ DATA 1 ）

应用数据区 1 ： 块 2 ～ 块 7 （DATA 1）

访问控制条件： 读 —— 无条件； 写 —— 认证 Key

●应用数据区 2 （ DATA 2 ）

应用数据区 2 ： 块 9 ～ 块 15 （DATA 2）

访问控制条件： 读 —— 认证 Key； 写 —— 认证 Key