JMY600 系列读写卡模块

MIFARE Ultralight C 卡操作指南

（Revision 1.04）

北京金木雨电子有限公司

2014/1/3

在使用本产品前请详细阅读本说明书，如果有任何疑问，请联系我们，我们会给您详尽的解答

目录

1 概述

本文详细介绍了使用JMY600 系列读卡模块操作MIFARE Ultralight C卡的操作方法和顺序以及基本卡片功能设计，您可以通过阅读本手册很快速地掌握MIFARE Ultralight C卡的使用和规划。本手册的使用对象为使用JMY600 系列RFID模块的程序员，我们也有通讯协议的例子代码，可以在随货的产品光盘上找到，也可以在金木雨的网站上找到。如果在编写程序中依然有任何的问题，请随时联系我们的技术支持。或发送电子邮件到：jinmuyu@vip.sina.com 我们会给您满意的答复。

2 主要性能指标

- 卡片向下完全兼容 MIFARE Ultralight，即可以完全代替 MIFARE Ultralight
- 容量为 192 字节
- 每张卡有唯一序列号，为 7 字节
- 具有防冲突机制，支持多卡操作
- 存储空间分为 48 块，每块 4 个字节，以块为存取单位
- 卡片拥有 3DES 加密的密码保护及访问控制
- 数据保存期为 10 年，可改写 10 万次，读无限次
- 工作温度：-20℃~50℃(湿度为 90%)
- 工作频率：13.56MHz
- 通信速率：106 Kbps
- 读写距离：大于 10 cm

3 卡片功能

MIFARE Ultralight C 卡是广泛使用的非接触 IC 卡，属于 3DES 加密的密码保护的存储卡，有比较高的安全性，价格低廉，非常适合用电子识别使用。也可以当作数据存储使用，但空间只有 192 字节。

4 存储结构

- MIFARE Ultralight C 存储器卡分为 48 个块，每个块的功能和存贮结构如下图所示：

逻辑块号	卡片内存，每块 4 字节，按字节表示
0	SN0，SN1，SN2，BCC0
1	SN3，SN4，SN5， SN6
2	BCC1，internal，Lock Byte 0，Lock Byte 1
3	OTP，OTP，OTP，OTP
4	USER DATA
5	USER DATA
6	USER DATA
	. USER DATA .
39	USER DATA
40	Lock byte 2，Lock Byte 3，rfu，rfu
41	CNT，CNT，rfu，rfu
42	AUTH0，rfu，rfu，rfu
43	AUTH1，rfu，rfu，rfu
44	Key，Key，Key，Key
45	Key，Key，Key，Key
46	Key，Key，Key，Key
47	Key，Key，Key，Key

- SN0-SN7 为卡片序列号
- BCC0 为 SN0-SN3 的 BCC 校验
- BCC1 为 SN3-SN7 的 BCC 校验
- Internal 为内部信息
- Lock Byte0-Lock Byte3 为功能锁定块，写入信息后可以锁定相应的数据块
- OTP 为数据单次写入功能区，每个位只能从 0 写到 1，不能再恢复成 0，默认值为 0
- USER DATA 是用户数据区，可以写入用户需要的任何数据，全部数据默认值为 0
- CNT 为 2 字节的计数器，只能单向增加操作，不能减，默认值为 0
- AUTH0 密钥认证功能设定，设定需要密钥认证后才能操作的的起始数据块号，合法的范围从 3 到 48，默认值为 48
- AUTH1 密钥认证功能设定，0：所有密钥保护数据区都需要认证才能读写；1：密钥保护数据区需要认证才能写，读不需要认证；默认值为 0
- Key，卡片的 3DES 认证密钥，默认值全部为 0
- rfu，保留供将来使用
- 以上内容的详细信息请参考卡片的 datasheet

5 卡片操作

5.1 主动读卡模式

主动读卡模式只能在 UART 或 RS232C 接口下使用，可用于电子识别，即卡片的序列号代表一定信息，如门禁系统，物品管理等。当卡片进入读卡模块的读卡范围后，读卡模块会在 UART 或 RS232C 上直接输出卡片序列号，从而达到管理的目的。

在此工作模式下，需要选择以下几个项目：

连续输出卡号或非连续

HEX 格式输出或 ASCII 格式输出

我们假定：连续输出卡号，以 HEX 格式输出，那么我们通过 TransPort 使用 JCP04 通讯协议给读卡模块发送配置命令：

- 配置：

  TransPort 中输入：1E 03

  实际端口发出指令：03 1E 03 1E

  实际端口收到：02 1E 1C

- 获得卡号输出：

  将 TransPort 关闭

  打开 sscom，选择正确端口，选择 19200bps，选择 HEX 显示

  将 MIFARE Ultralight C 卡靠近读卡天线，如果有蜂鸣器，此时蜂鸣器会鸣响

  在窗口中就会连续接收到这样的数据：0C 20 04 23 74 E1 ED 25 80 44 00 00 92

  这是符合 JCP04 通讯协议的数据包，在此使用 JCP04 的原因是数据包较短。

  数据包中，0C 是长度字，20 是寻卡命令字，04 23 74 E1 ED 25 80 是卡片序列号，44 00 是 ATQA，00 是 SAK，92 是校验字。

  每张 MIFARE Ultralight C 卡的序列号是唯一的，可以作为识别使用。

在做过以上实验后，请将模块恢复默认设置以方便后续实验：

- 恢复默认设置：

  TransPort 中输入：0F 52 45 53 45 54

  实际端口发出指令：07 0F 52 45 53 45 54 5D

  实际端口收到：02 0F 0D

模块重新上电后，即恢复了默认设置。

5.2 被动读卡模式

在操作 MIFARE Ultralight C 的卡片的过程中，如果使用了 3DES 加密的密钥认证功能，就不能使用 JMY600 的自动寻卡模式。使用 JMY600 的自动寻卡模式操作 MIFARE Ultralight C 卡片需要将模块的 ICC 引脚连接到用户系统中，开启自动寻卡后，此时模块的读卡操作功能被禁止，当卡片进入天线区域时 ICC 会出现低电平，此时可以直接发送读写卡的指令对卡片进行操作而无需发送寻卡命令。

对于无法将 ICC 连接至用户系统或使用了 3DES 加密的密钥认证功能的情况，请使用 0x20

命令寻卡，寻到卡片后，可以对卡片进行操作了。

取一张新卡，全部块不认证都可以读写，做如下实验，在此选择 JCP05 通讯协议，将卡片放到天线上，可以发送如下命令：

- 寻卡：

  TransPort 中输入：20 00

  实际端口发出指令：00 05 00 20 00 25

  实际端口收到：00 0E 01 20 04 23 74 E1 ED 25 80 44 00 00 91

- 写块：

  TransPort 中输入：42 05 55 55 55 55

  实际端口发出指令：00 09 00 42 05 55 55 55 55 4E

  实际端口收到：00 04 01 42 47

- 读块：

  TransPort 中输入：41 05

  实际端口发出指令：00 05 00 41 05 41

  实际端口收到：00 14 01 41 55 55 55 55 00 00 00 00 00 00 00 00 00 00 00 00 54

以上部分是基本的不认证密钥的读写操作，以下写入密钥并启动认证：

- 写入密钥：

  TransPort 中输入：42 2C 00 00 00 00

  实际端口发出指令：00 09 00 42 2C 00 00 00 00 67

  实际端口收到：00 04 01 42 47

  TransPort 中输入：42 2D 00 00 00 00

  实际端口发出指令：00 09 00 42 2D 00 00 00 00 66

  实际端口收到：00 04 01 42 47

  TransPort 中输入：42 2E 00 00 00 00

  实际端口发出指令：00 09 00 42 2E 00 00 00 00 65

  实际端口收到：00 04 01 42 47

  TransPort 中输入：42 2F 00 00 00 00

  实际端口发出指令：00 09 00 42 2F 00 00 00 00 64

  实际端口收到：00 04 01 42 47

- 写入权限：

  权限默认为数据保护区的数据读写都需要认证，在此不需要做修改。

- 写入密钥管控范围：

  TransPort 中输入：42 2B 20 00 00 00

  实际端口发出指令：00 09 00 42 2B 20 00 00 00 40

  实际端口收到：00 04 01 42 47

- 重新寻卡

  见前面寻卡操作

- 认证密钥：

  TransPort 中输入：43 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

  实际端口发出指令：00 14 00 43 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 57

  实际端口收到：00 04 01 43 46

- 读取被密钥保护的块：

  TransPort 中输入：41 20

  实际端口发出指令：00 05 00 41 20 64

实际端口收到：00 14 01 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 54

- 写入被密钥保护的块：

  TransPort 中输入：42 20 01 02 03 04

  实际端口发出指令：00 09 00 42 20 01 02 03 04 6F

  实际端口收到：00 04 01 42 47

- 再次读取被密钥保护的块：

  TransPort 中输入：41 20

  实际端口发出指令：00 05 00 41 20 64

  实际端口收到：00 14 01 41 01 02 03 04 00 00 00 00 00 00 00 00 00 00 00 00 50