JMY600 系列读写卡模块

MIFARE 1 卡操作指南

（Revision 1.13）

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 1 卡片的方法和顺序，您可以通过阅读本手册很快速地掌握MIFARE 1 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

- 容量为 1K 字节
- 每张卡有唯一序列号，为 4 字节
- 具有防冲突机制，支持多卡操作
- 存储空间分为 16 个扇区，每个扇区为 4 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
- 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 1 卡是广泛使用的非接触 IC 卡，属于逻辑加密的存储卡，价格低廉，非常适合用做小额电子钱包使用。也可以当作数据存储使用，但空间只有 1K 字节。

4 存储结构

- M1 卡分为 16 个扇区，每个扇区由 4 块（块 0、块 1、块 2、块 3）组成，也将 16 个扇区的 64 个块按逻辑地址编号为 0~63，存贮结构如下图所示：

扇区编号	扇区内块号	卡片内存	块类型	逻辑块号
Sector 0	Block 0	序列号、厂商代码	Data block	0
	Block 1		Data block	1
	Block 2		Data block	2
	Block 3	密码 A 存取控制 密码 B	Sector trailer	3
Sector 1	Block 0		Data block	4
	Block 1		Data block	5
	Block 2		Data block	6
	Block 3	密码 A 存取控制 密码 B	Sector trailer	7
		⋮		
Sector 15	Block 0		Data block	60
	Block 1		Data block	61
	Block 2		Data block	62
	Block 3	密码 A 存取控制 密码 B	Sector trailer	63

- 第 0 扇区的块 0（即逻辑地址 0 块），它用于存放序列号和厂商代码，已经固化，不可更改。
- 每个扇区的块 0、块 1、块 2 为**数据块**，可用于存贮数据。

  数据块可作两种应用：

  ★ 用作一般的数据保存，可以进行**读**、**写**操作。

  ★ 用作数据值，可以进行**初始化值**、**加值**、**减值**、**读值**操作。
- 每个扇区的块 3 为**控制块**，包括了密码 A、存取控制、密码 B。具体结构如下：

FF FF FF FF FF FF	FF 07 80 69	FF FF FF FF FF FF
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。存取控制为 4 个字节，共 32 位，扇区中的每个块（包括数据块和控制块）的存取条件是由密码和存取控制共同决定的，有关存取条件的设定，用户可以查看卡片的 datasheet，或使用我们提供的密码存取条件设定工具来设定，这将非常容易。

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 1 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：09 20 8D CE F8 01 04 00 00 97

  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，09 是长度字，20 是寻卡命令字，8D CE F8 01 是卡片序列号，04 00 是 ATQA，00 是 SAK，97 是校验字。

  每张 MIFARE 1 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

使用 JMY600 的自动寻卡模式操作 MIFARE 1 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，默认密钥为 FFFFFFFFFFFF，A 密钥拥有全部权限，B 密钥没有任何权限，

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 0B 01 20 BD 32 30 63 04 00 08 FA

寻到卡后，以下指令都可执行，除钱包应先初始化再读之外，其他指令不分先后

- 读卡一块：

  TransPort 中输入：21 00 00 FF FF FF FF FF FF

  实际端口发出指令：00 0C 00 21 00 00 FF FF FF FF FF FF 2D

  实际端口收到：00 14 01 21 BD 32 30 63 DC 08 04 00 62 63 64 65 66 67 68 69 38

- 读卡多块：

  TransPort 中输入：2A 00 01 02 FF FF FF FF FF FF

  实际端口发出指令：00 0D 00 2A 00 01 02 FF FF FF FF FF FF 24

  实际端口收到：00 24 01 2A 05 03 02 01 FA FC FD FE 05 03 02 01 02 FD 02 FD 05 03 02 01 FA FC FD FE 05 03 02 01 02 FD 02 FD 0F

- 写卡一块：

  TransPort 中输入：22 00 01 FF FF FF FF FF FF 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

  实际端口发出指令：00 1C 00 22 00 01 FF FF FF FF FF FF 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 3F

  实际端口收到：00 04 01 22 27

- 写卡多块：

  TransPort 中输入：2B 00 01 02 FF FF FF FF FF FF 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F

  实际端口发出指令：00 2D 00 2B 00 01 02 FF FF FF FF FF FF 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 05

  实际端口收到：00 04 01 2B 2E

- 初始化钱包：

  TransPort 中输入：23 00 02 FF FF FF FF FF FF 04 03 02 01

  实际端口发出指令：00 10 00 23 00 02 FF FF FF FF FF FF 04 03 02 01 35

  实际端口收到：00 04 01 23 26

- 读钱包余额：

  TransPort 中输入：24 00 02 FF FF FF FF FF FF

  实际端口发出指令：00 0C 00 24 00 02 FF FF FF FF FF FF 2A

  实际端口收到：00 08 01 24 04 03 02 01 29

- 钱包加值：

  TransPort 中输入：25 00 02 FF FF FF FF FF FF 01 00 00 00

  实际端口发出指令：00 10 00 25 00 02 FF FF FF FF FF FF 01 00 00 00 36

  实际端口收到：00 04 01 25 20

- 钱包扣款：

  TransPort 中输入：26 00 02 FF FF FF FF FF FF 01 00 00 00

  实际端口发出指令：00 10 00 26 00 02 FF FF FF FF FF FF 01 00 00 00 35

  实际端口收到：00 04 01 26 23

- 备份钱包：

TransPort 中输入：27 00 02 01 FF FF FF FF FF FF 29

实际端口发出指令：00 0E 00 27 00 02 01 FF FF FF FF FF FF 29 03

实际端口收到：00 04 01 27 22

- 当前 MIFARE 1 卡休眠：

  TransPort 中输入：28

  实际端口发出指令：00 04 00 28 2C

  实际端口收到：00 04 01 28 2D