JMY600 系列读写卡模块

MIFARE Ultralight EV1 卡操作指南

（Revision 1.00）

北京金木雨电子有限公司

2014/5/21

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 EV1 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 EV1 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 80 字节或 164 字节，相应的用户空间为字节 48 字节或 128 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
- 存储空间以块为单位存取单位，每块 4 个字节
- 3 个独立的单向递增计数器
- 基于 ECC 的原厂签名验证功能
- 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 EV1 卡是广泛使用的非接触 IC 卡，属于带有密码保护的存储卡，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，但空间只有较小。

4 存储结构

- MF0UL1(MIFARE Ultralight EV1 的 80 字节版本)存储器卡分为 19 个块，每个块的功能和存贮结构如下图所示：（更详细的内容请参考卡片的 datasheet）

Page Adr		Byte number within a page				
Dec	Hex	0	1	2	3	Description
0	0h	serial number				Manufacturer data and lock bytes
1	1h	serial number				
2	2h	serial number	internal	lock bytes		
3	3h	OTP	OTP	OTP	OTP	One Time Programmable
4	4h	user memory				User memory pages
5	5h					
...	...					
14	Eh					
15	Fh					
16	10h	CFG0				Configuration pages
17	11h	CFG1				
18	12h	PWD				
19	13h	PACK		RFUI		
		One-Way counters [1]				Counter pages

aaa-006275

(1) counter pages are only accessible with READ_CNT and INCR_CNT commands

Fig 5. Memory organization MF0UL11

- MF0UL2(MIFARE Ultralight EV1 的 164 字节版本)存储器卡分为 40 个块，每个块的功能和存贮结构如下图所示：

Page Adr		Byte number within a page				
Dec	Hex	0	1	2	3	Description
0	0h	serial number				Manufacturer data and lock bytes
1	1h	serial number				
2	2h	serial number	internal	lock bytes		
3	3h	OTP	OTP	OTP	OTP	One Time Programmable
4	4h	user memory				User memory pages
5	5h					
...	...					
34	22h					
35	23h					
36	24h	lock bytes			RFUI	Lock bytes
37	25h	CFG0				Configuration pages
38	26h	CFG1				
39	27h	PWD				
40	28h	PACK		RFUI		
		one-way counters [1]				Counter pages

aaa-006276

(1) counter pages are only accessible with READ_CNT and INCR_CNT commands

Fig 6. Memory organization MF0UL21

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 EV1 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 EV1 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

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 42 6A 72 9F 35 80 44 00 00 1F

- 读块：

  TransPort 中输入：41 04

  实际端口发出指令：00 05 00 41 04 40

  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

  得到的 16 字节信息是 4.5.6.7 块的数据
- 写块：

  TransPort 中输入：42 04 44 44 44 44

  实际端口发出指令：00 09 00 42 04 44 44 44 44 4F

  实际端口收到：00 04 01 42 47

  数据块可以随意读写，其他的功能块在写入之前要充分阅读原厂说明书。
- 再次读块：

  TransPort 中输入：41 04

  实际端口发出指令：00 05 00 41 04 40

  实际端口收到：00 14 01 41 44 44 44 44 00 00 00 00 00 00 00 00 00 00 00 00 54
- 快速读取数据：

  使用快速读取指令一次读取 16 块数据

  TransPort 中输入：47 04 10

  实际端口发出指令：00 06 00 47 04 10 55

  实际端口收到：00 38 01 47 44 44 44 44 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF 81

- 读计数器：

  TransPort 中输入：48 00

  实际端口发出指令：00 05 00 48 00 4D

  实际端口收到：00 07 01 48 00 00 00 4E

  这是一个新卡，计数器 0 的值是：00 00 00
- 计数器递增：

  计数器 0 递增 1

  TransPort 中输入：49 00 01 00 00

  实际端口发出指令：00 08 00 49 00 01 00 00 40

  实际端口收到：00 07 01 48 00 00 00 4E
- 再次读计数器：

  TransPort 中输入：48 00

  实际端口发出指令：00 05 00 48 00 4D

  实际端口收到：00 07 01 48 01 00 00 4F

  计数器已经递增
- 读取单向计数器的 Tearing 事件：

  TransPort 中输入：8C 00

  实际端口发出指令：00 05 00 8C 00 89

  实际端口收到：00 05 01 8C BD 35

- 认证密钥：

  TransPort 中输入：4A FF FF FF FF

实际端口发出指令：00 08 00 4A FF FF FF FF 42

实际端口收到：00 06 01 4A 00 00 4D

认证密钥后，就可以读写被密钥保护的块

- 读卡片版本号：

  TransPort 中输入：46

  实际端口发出指令：00 04 00 46 42

  实际端口收到：00 0C 01 46 00 04 03 01 01 00 0B 03 44

- 读取卡片的原厂签名：

  TransPort 中输入：4B

  实际端口发出指令：00 04 00 4B 4F

  实际端口收到：00 24 01 4B E2 7A E8 10 83 D2 AE 81 A1 8A 9C D1 D6 F9 9F DD 22 CB 5C 31 06 AC DB A8 8E 1D 14 FE D8 2C D0 18 63