JMY350B_370B 门禁读写器

用户手册

(Revision 1.5)

北京金木雨电子有限公司

2021/4/6

目录

文件修改记录

日期	版本号	修改内容
---	V1.0	新建文档
2019.12.22	V1.1	添加对 BLE 主机模式的介绍
2020.04.15	V1.2	添加对 BLE 从机模式介绍
2021.03.04	V1.3	修改设置读卡器参数指令介绍
2021.03.23	V1.4	修改管脚定义
2021.04.06	V1.5	修改写入脚本信息指令的限定描述

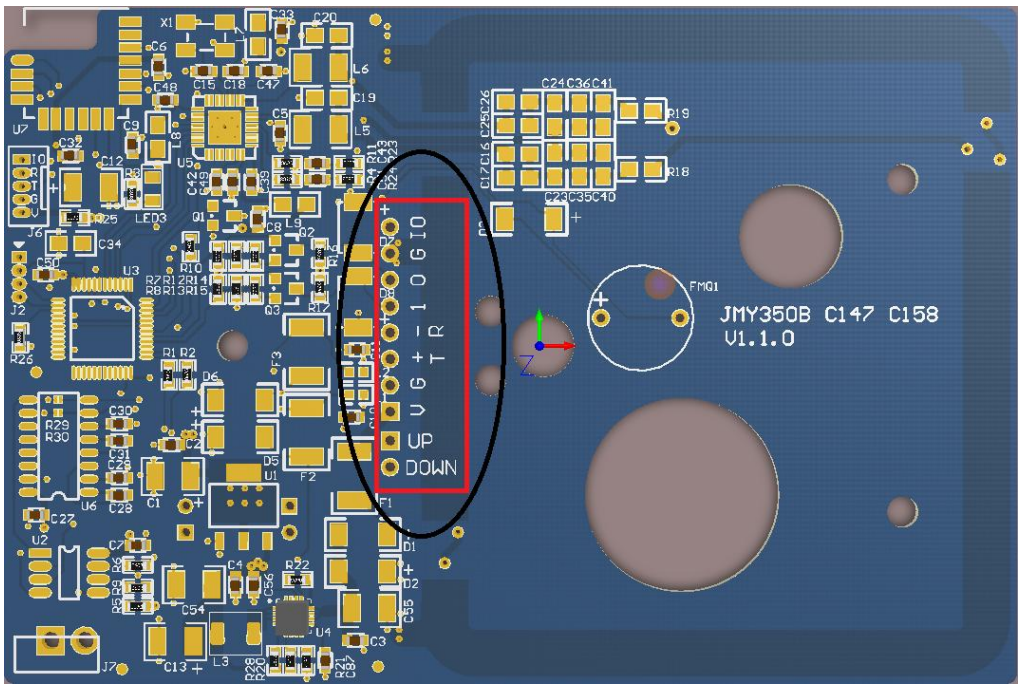
1 特点

- 可读卡型： ISO14443-4 TYPE A+B
- 供电电压： DC 12V
- 接口： RS485，Wiegand
- 最大功耗： 100mA
- 读卡距离： 0-8cm(根据卡种类有所不同)
- ISP： 支持
- 适用环境： -25~+85 ℃
- 储存环境： -40 ~ +125 ℃

2 规格和引脚

2.1 JMY350B 引脚定义及图示

Pin1	Pin2	Pin3	Pin4	Pin5	Pin6	Pin7	Pin8	Pin9	Pin10
Down	Up	+12V	GND	D+	D-	Bit1	Bit0	GND	IO
		红	黑	黄	绿	白	褐		
开盖保护		电源		RS485		Wiegand		Onekey	
选用		必备		两种接口都支持，默认 RS485				客户定制	



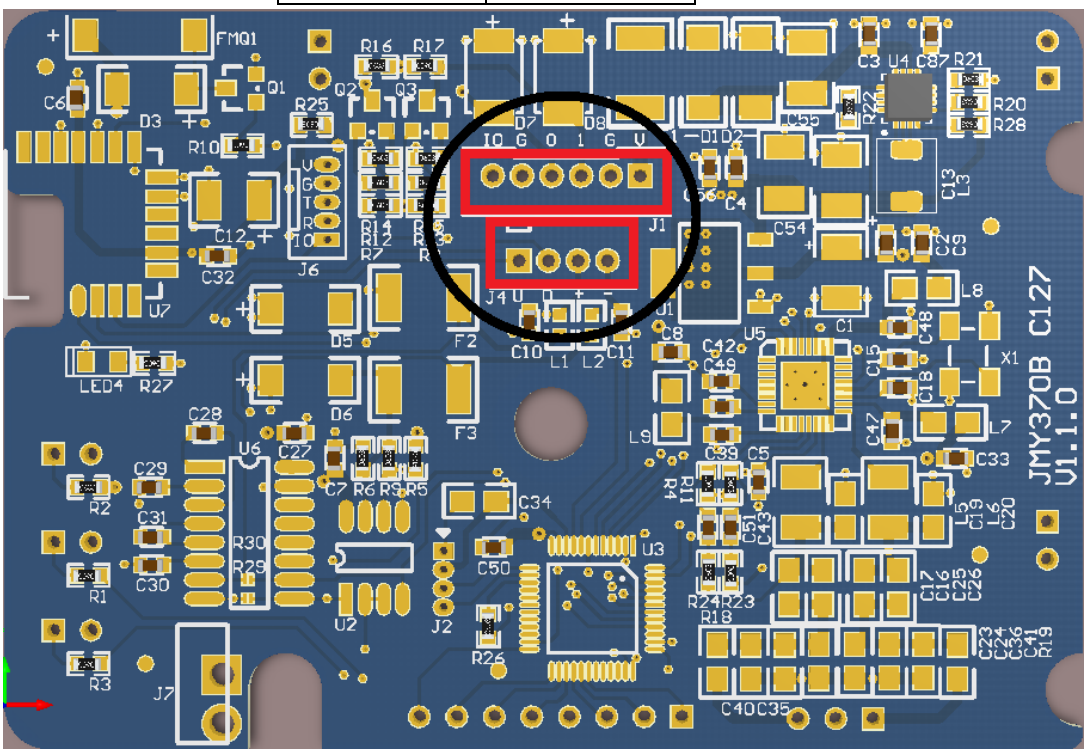
2.2 JMY370B 引脚及图示

J1:

Pin1	Pin2	Pin3	Pin4	Pin5	Pin6
IO	GND	Bit0	Bit1	GND	+12V
		褐	白	黑	红
Onekey		Wiegand		电源	
客户定制		选用		必备	

J4:

Pin1	Pin2	Pin3	Pin4
Up	Down	D+	D-
		黄	绿
开盖保护		RS485	
选用		默认选用	



3 通讯协议

3.1 RS485 协议

3.1.1 规格

通信协议采用字节为单位，接收和发送数据都是十六进制格式，通信参数如下：

- 波特率：19200 bps
- 数据位：8 位
- 停止位：1 位
- 奇偶校验：无
- 流控制：无

3.1.2 JCP04 数据格式

长度字	命令字	数据域	校验字

- 长度字：1 字节，指明从长度字到数据域最后一字节的字节数
- 命令字：1 字节
- 数据域：长度由命令类型决定，长度为 0x00~0xFC。
- 校验字：1 字节，从长度字到数据域最后一字节的逐字节异或（XOR）值

3.1.3 JCP04 数据返回格式

- 成功返回：

长度字	命令字	数据域	校验字

- 失败返回：

长度字	命令字取反	校验字

3.1.4 JCP05 数据格式

长度字	通讯地址	命令字	数据域	校验字

- 长度字：2 字节，指明从长度字到数据域最后一字节的字节数，高字节在前，取值范围为：0x0004～0x01FE。
- 通讯地址：1 字节，多机通讯的设备地址，1 为设备出厂默认地址，0 为群呼地址
- 命令字：1 字节
- 数据域：数据长度由命令字决定，长度为 0 至 506 字节，根据所使用的处理器不同，部分型号会小于 506 字节。
- 校验字：1 字节，从长度字到数据域最后一字节的逐字节异或（XOR）值

3.1.5 JCP05 数据返回格式

- 成功返回：

长度字	通讯地址	命令字	数据域	校验字

●失败返回：

长度字	通讯地址	命令字取反	校验字

3.2 Wiegand 协议

支持 Wiegand26/34/42/50。

4 命令说明

4.1 命令列表

命令字	说明
0x18	配置设备地址
0x20	ISO14443 Type A 寻卡指令
0x30	ISO14443 Type A CPU 卡复位指令
0x31	ISO14443 Type A CPU 卡通信指令
0x60	ISO14443 Type B CPU 卡复位指令
0x61	ISO14443 Type B CPU 卡 COS 通信指令
0xA0	写入脚本
0xA1	读出脚本
0xA2	清除脚本
0xA5	设置读卡器参数
0xA8	读取 8 字节加密随机数
0xA9	设置通信密钥
0xAF	保存读卡器参数
0xB0	蜂鸣器和 LED 控制
0xB1	BLE 命令使能
0xB2	BLE 命令禁止
0xB3	设定主机模式扫描范围
0xB4	主机模式扫描 MAC 地址
0xB5	复位蓝牙模块
0xB6	硬件复位蓝牙模块
0xB7	设定主机模式自动扫描使能
0xB8	蓝牙工作模式设定
0xB9	蓝牙广播名称设置
0xF1	版本信息

4.2 命令介绍

4.2.1 设置设备地址

上位机发送：

帧头	0x18	Addr	校验字

Addr：1 字节，0x01~0xFF，不允许为 0x00，默认为 0x01。

模块回应成功：

帧头	0x18	校验字

模块回应失败：

帧头	0xE7	校验字

4.2.2 ISO14443 Type A 寻卡

上位机发送：

帧头	0x20	参数	校验字

参数: 0x26 寻找天线区域未休眠的卡片

0x52 寻找天线区域所有卡片

模块回应成功：

帧头	0x20	SNR	校验字

SNR: 4，7 或 10 字节卡片序列号

模块回应失败：

帧头	0xDF	校验字

4.2.3 ISO14443 Type A CPU 卡复位

上位机发送：

帧头	0x30	校验字

模块回应成功：

帧头	0x30	复位信息	校验字

复位信息: 按照 ISO14443-4 描述的复位回复信息。

模块回应失败：

帧头	0xCF	校验字

4.2.4 ISO14443 Type A CPU 卡通信

上位机发送：

帧头	0x31	COS 命令	校验字

COS 命令： 符合 ISO14443-4 的通信命令。

模块回应成功：

帧头	0x31	COS 回复	校验字

模块回应失败：

帧头	0xCE	校验字

示例 JCP05：

发送：0x0009 00 31 00 84 00 00 08 B4

返回：0x000E 01 31 B9 89 3A B0 16 40 7E D0 90 00 EC

4.2.5 ISO14443 Type B CPU 卡复位

上位机发送：

帧头	0x60	模式	校验字

模式:1 字节，0x00 WUPB; 0x01:REQB; 其他值保留

模块回应成功：

帧头	0x60	复位信息	校验字

复位信息: 按照 ISO14443-4 描述的复位回复信息。

模块回应失败：

帧头	0x9F	校验字

4.2.6 ISO14443 Type B CPU 卡通信

上位机发送：

帧头	0x61	COS 命令	校验字

模块回应成功：

帧头	0x61	COS 回复	校验字

模块回应失败：

帧头	0x9E	校验字

4.2.7 写入脚本信息

写入脚本信息之前，需要发送 A2h 指令(清除读卡器参数和脚本数据指令)获取权限。重新上电，权限失效。

上位机发送：

帧头	0xA0	DATA	校验字

DATA：脚本命令

该文件只描述串口通讯结构，具体脚本信息结构，及使用方法请查阅“脚本协议文件”。

模块回应成功：

帧头	0xA0	校验字

模块回应失败：

帧头	0x5F	校验字

4.2.8 读出脚本信息

上位机发送：

帧头	0xA1	INDEX	校验字

INDEX：指定脚本命令序号

模块回应成功：

帧头	0xA1	DATA	校验字

DATA: 脚本命令

该文件只描述串口通讯结构，具体脚本信息结构，及使用方法请查阅“脚本协议文件”。

模块回应失败：

帧头	0x5E	校验字

4.2.9 清除读卡器参数和脚本数据

上位机发送：

帧头	0xA2	Flag	校验字

Flag：1 字节，0xFF。

模块回应成功：

帧头	0xA2	校验字

模块回应失败：

帧头	0x5D	校验字

4.2.10 设置读卡器参数

设置读卡器寻卡，脚本执行，输出功能等。

上位机发送：

帧头	0xA5	DATA	校验字

DATA 3 字节：

	位	说明

DATA[0]	Bit7	RFU
	Bit6	1=Enable; 0=Disable;　加密方式输出数据；
	Bit5	1=Enable; 0=Disable;　RS485 接口输出数据；
	Bit4	1=Enable; 0=Disable;　WieGand 接口输出数据；
	Bit3-bit0	3=WieGand26 或 RS485 三字节 4=WieGand34 或 RS485 四字节 5=WieGand42 或 RS485 五字节 6=WieGand50 或 RS485 六字节
DATA[1]	Bit7	1=Enable; 0=Disable;　自动寻卡功能
	Bit6	1=Enable; 0=Disable;　自动寻按键功能
	Bit5	1=Enable; 0=Disable;　使用脚本
	Bit4-bit0	RFU
DATA[2]		RFU
DATA[3]		设备地址

模块回应成功：

帧头	0xA5	校验字

模块回应失败：

帧头	0x5A	校验字

4.2.11　保存读卡器参数

上位机发送：

帧头	0xAF	校验字

模块回应成功：

帧头	0xAF	校验字

模块回应失败：

帧头	0x50	校验字

4.2.12 读取 8 字节加密随机数

读取 8 字节的加密随机数，默认的读卡器密钥为 4A494E4D55595520。该密钥是固定值，请妥善保管。

上位机发送：

帧头	0xA8	校验字

模块回应成功：

帧头	0xA8	加密随机数	校验字

加密随机数：　8 字节　用于读写器输出”加密数据功能”所用的 DES 加密密钥。

模块回应失败：

帧头	0x57	校验字

4.2.13 设置通信密钥

上位机发送：

帧头	0xA9	加密数据	校验字

加密数据： 16 字节 用于读写器输出“加密数据功能”所用的 DES 加密密钥。

模块回应成功：

帧头	0xA9	校验字

模块回应失败：

帧头	0x56	校验字

4.2.14 控制蜂鸣器和 LED

上位机发送：

帧头	0xB0	DATA	校验字

DATA[0]： Beep 和 LED 控制

Bit5 Green LED 反向显示

Bit4 Red LED 反向显示

Bit3 RFU

Bit2 Beep 控制

Bit1 Green LED 控制

Bit0 Red LED 控制

DATA[1-2]： 高字节在前，蜂鸣器控制时间(单位 10ms)。

DATA[3-4]： 高字节在前，绿色 LED 控制时间(单位 10ms)。

DATA[5-6]： 高字节在前，红色 LED 控制时间(单位 10ms)。

模块回应成功：

帧头	0xB0	校验字

模块回应失败：

帧头	0x4F	校验字

例：

红色反向显示，绿色正向，蜂鸣器蜂鸣。

发送：09 B0 17 00 0A 00 0A 00 0A A4

4.2.15 BLE 命令使能

注：在 BLE 模块复位或 BLE 命令禁止后，需要重新进入 BLE 命令模式，才可以发送 BLE 配置指令。默认使能。

上位机发送：

帧头	0xB1	校验字

模块回应成功：

帧头	0xB1	校验字

模块回应失败：

帧头	0x4E	校验字

4.2.16 BLE 命令禁止

注：使能 BLE 功能后，才可以发送该指令。

上位机发送：

帧头	0xB2	校验字

模块回应成功：

帧头	0xB2	校验字

模块回应失败：

帧头	0x4D	校验字

4.2.17 软复位蓝牙接口

注：需要使能 BLE 功能后，才可以发送该指令

上位机发送：

帧头	0xB5	校验字

模块回应成功：

帧头	0xB5	校验字

模块回应失败：

帧头	0x4A	校验字

4.2.18 硬复位蓝牙接口

上位机发送：

帧头	0xB6	校验字

模块回应成功：

帧头	0xB6	校验字

模块回应失败：

帧头	0x49	校验字

4.2.19 设定蓝牙工作模式

上位机发送：

帧头	0xB8	Mode	校验字

Mode: 0x4D – Master（出厂默认）

0x53 - Slave

模块回应成功：

帧头	0xB8	校验字

模块回应失败：

帧头	0x47	校验字

4.2.20 主机模式下设定扫描范围

注：仅主机模式有效。

上位机发送：

帧头	0xB3	Signal	校验字

Signal: 扫描蓝牙范围。取值范围 0~0x40，默认最大。

模块回应成功：

帧头	0xB3	校验字

模块回应失败：

帧头	0x4C	校验字

4.2.21 主机模式下扫描蓝牙设备

注：需要使能 BLE 命令功能后，才可以发送改指令。仅主机模式有效。

上位机发送：

帧头	0xB4	校验字

模块回应成功：

帧头	0xB4	校验字

模块回应失败：

帧头	0x4B	校验字

4.2.22 设定主机模式下自动扫描使能

注：仅主机模式有效。

上位机发送：

帧头	0xB7	使能	校验字

使能：1 字节

	位	说明
使能	Bit7	1=Enable; 0=Disable;　自动扫描使能；
	Bit6~bit4	默认必须为 0
	Bit3~bit0	自动扫描间隔，单位秒，（最小 1 秒，默认 10 秒）

模块回应成功：

帧头	0xB7	校验字

模块回应失败：

帧头	0x48	校验字

4.2.23 设定蓝牙广播名称

注：使能 BLE 命令功能后，才可以发送该指令

上位机发送：

帧头	0xB9	Name	校验字

Name: 十六进制，长度限制（1~15 字节）。

模块回应成功：

帧头	0xB9	校验字

模块回应失败：

帧头	0x46	校验字

4.2.24 版本信息

上位机发送：

帧头	0xF1	校验字

模块回应成功：

帧头	0xF1	版本信息	校验字

版本信息：包括软件版本编号和日期，返回的信息均为 ASCII 码。

模块回应失败：

帧头	0x0E	校验字

5 加密输出功能

该功能主动输出固定 8 字节的 DES 加密数据。服务端对 8 字节数据做 DES 解密即可还原真实数据,密码数据是加密的 16 字节。

5.1 数据格式

5.1.1 卡片 UID

4Byte	2Byte	1Byte	1Byte
卡片 UID	随机数	指示码	校验

卡片 UID： 读卡器读取到的卡片 UID。
随机数： DES 加密得到 8 字节不同结果。
指示码： 0x01
校验码： 前边 7 字节做异或校验

例如：

卡片 UID 是 12345678；随机是 0000；指示码 01；校验码 09；
8 字节序列：1234567800000109

5.1.2 门铃按键

1Byte	5Byte	1Byte	1Byte
数据码	随机数	指示码	校验

数据码： 当前按键状态，Bit0=0 按键按下,其它位默认为 1。
随机数： DES 加密得到 8 字节不同结果。
指示码： 0x81
校验码： 前边 7 字节做异或校验

例如：

门铃按下是 0xFE；随机是 0x0000000000；指示码 81；校验码 7F；
8 字节序列：FE0000000000817F

5.1.3 密码

8Byte	6Byte	1Byte	1Byte
密码	随机数	指示码	校验

密码： 8 字节密码
随机数： 6 字节随机数。
指示码： 0x08
校验码： 前边 15 字节做异或校验

说明：

密码空间预留 8 字节，密码长度为 4~8 字节，长度补足 8 字节，末尾补 0

示例：

Key: 1122334455667788

密文: 178F59F8578E0D3F FA2AEF9C7CA5716E

明文: 0102030405060708 1B2625202F2A 08 3D

密文: 0806C51B5B060577 B003436BED45CEA6

明文: 0009080700000000 3A3530330E0A 08 06

5.1.4 BleMAC

6Byte	1Byte	1Byte
数据码	指示码	校验

数据码： 6 字节 BleMAC 地址

指示码： 0x10

校验码： 前边 7 字节做异或校验

5.2 数据加密和解密

以读卡器输出卡片 UID 数据为例：

假设密钥： 123456789ABCDEF0

数据： 1234567800000109

加密结果： E87510B61BF92C02

服务器数据解密：

服务器接收数据：E87510B61BF92C02

解密结果：1234567800000109

6 部分协议

密钥设置流程

第一步：读取加密随机数

发送： 02 A8 AA

接收： 0A A8 15FD10A8EA65723D 32

15FD10A8EA65723D 八字节加密随机数，解密数据还原为 AAAAAAAAAAAAAAAA。

第二步：配置修改的数据传输密钥

假如要设置的数据传输密钥为 123456789ABCDEF0

那么要发送的原始数据为 AAAAAAAA 12345678 AAAAAAAA 9ABCDEF0.

第三步：加密数据

使用读卡器密钥对 16 字节的原始设置数据做两次加密处理。

得到的加密数据为 efaa9df287711279fae5201cb8639038

第四步：设置数据加密密钥

发送： 12 A9efaa9df287711279fae5201cb8639038 5C

接收： 02 A9 AB

接收到成功说明加密数据密钥设置完成，至此密钥成功被设置。