深圳市长城物联科技有限公司

串行通信协议文档

版本： V1.2

日期： 20210705

拟定人： 蔡承恩

审核人：

修订记录

日期	版本	修订内容	修订人
20200319	V1.0	制定协议	蔡承恩
20201123	V1.1	增加修改部分指令	蔡承恩
20210705	V1.2	精简完善部分指令	蔡承恩

1 文档说明

1.1 编写目的

此文档主要用于详细说明长城物联科技有限公司出品的读卡模块、读卡器、发卡器等产品所使用的通信方式以及通信协议。其中包括 TTL、RS232、RS485、USB 等接口。产品可能支持一个或者多个接口，具体参考产品说明书。

1.2 关键说明

此文档中可能包含的关键词有：mifare 卡、desfire 卡、cpu 卡、扇区、数据块、应用、密码、读卡流程。

此文档中的读卡设备已简化大部分卡片操作流程，但是操作卡片依然需要相关的卡片知识。

2 通信接口设置说明

2.1 硬件接口连接方式

2.1.1 TTL 接口

硬件 TTL，0V - 5V 电压，交叉连接，读卡设备上的 RXD 线连接到主机上的 TXD，读卡设备上的 TXD 线连接到主机上的 RXD。

2.1.2 RS232 接口

硬件 RS232，-12V - +12V 电压，交叉连接，读卡设备上的 RXD 线连接到主机上的 TXD，读卡设备上的 TXD 线连接到主机上的 RXD。

2.1.3 RS485 接口

硬件 RS485，差分信号，0V - 6V 电压，直连，读卡设备上的 485+/A 线连接到主机上的 485+/A，读卡设备上的 485-/B 线连接到主机上的 485-/B。

2.1.4 USB 接口

硬件 USB 为 2.0 版本，差分信号，0V - 5V 电压，直连，D+对应连接 D+，D-对应连接 D-。

2.2 软件设置

2.2.1 TTL/RS232/RS485 端口设置

主板上的软件需要找到连接模块对应的端口(COM)，然后简单的配置端口即可正常和模块进行通信。配置参数如下：

参数	描述
波特率	可选: 9600, 19200, 38400, 57600, 115200
数据位	固定: 8 bits
起始位	固定: 1 Bits
停止位	固定: 1 bit.
校验位	可选: Odd, Even, None

下面为默认配置：

波特率	数据位	起始位	停止位	校验位
115200	8	1	1	None

2.2.2 USB 端口通信设置

USB 设备为 HID 通信模式。

HID 通信端点：

通信端点	通信方向
0x82	读卡设备发往主机
0x02	主机发往读卡设备

3 通信协议说明

3.1 数据包格式

3.1.1 命令包格式

一包完整的数据包含有包头、类型、地址、数据长度、命令字、数据、校验、包尾。其中命令包是由主机发送到模块，返回包是由模块返回主机。

发送包格式（主机到模块）：

STX	DEVICE TYPE	DEVICE NUM	DATA LENGTH	CMD	DATA [0..N]	XOR	ETX

返回包格式（模块到主机）：

STX	DEVICE TYPE	DEVICE NUM	DATA LENGTH	STATUS	DATA [0..N]	XOR	ETX

3.1.2 命令包中字段描述

字段	长度	描述	备注
STX	1	0xAB－包头。标准控制字节. 表示一个数据包的开始	
DEVICE TYPE	1	设备类型	设备类型 0 则表示不论什么设备都需要响应命令。
DEVICE NUM	1	设备地址，在多机通讯所必需，模块在收到数据包后判断包内的地址与自身预设地址是否相符，相符才会响应。	读卡设备会响应任何带 0x00 和 0xFF 地址的数据包(不进行地址判断)。

DATALENGTH	2	数据包中数据字节的长度.包括 CMD/STATUS 和 DATA,但不包括 XOR. LENGTH=字节数(CMD/STATUS + DATA[0-N])	
CMD/STATUS	1	CMD: 主机发送至读卡设备 STAUS：读卡设备返回主机，指示命令处理结果	分别对应 3.2 命令列表和 3.3 状态列表
DATA [0-N]	N	这是一个长度与命令字有关的数据流。也有部分命令不需要附加数据.	
XOR	1	8bits 的校验字节.它包括除 STX, ETX 外所有字节的异或校验.	
ETX	1	0xBA-包尾。标准控制字节，表示数据包的结束.	

3.2 命令列表

命令列表		
命令码	**名称**	**描述**
通信设备		
0x0B	dev_GetInfo	读取设备信息
0x0C	dev_UpFirmware	更新固件
0x0E	dev_EnterIAP	进入 IAP 模式
0x0F	dev_ExitIAP	退出 IAP 模式
0x10	dev_SetBaud	设置通信速率
0x11	dev_SetAddr	设置设备编号
0x16	dev_SetWorkMode	设置设备的工作模式
0x17	dev_Restart	重启设备
0x1A	dev_SwitchRF	开关射频信号
0x1B	dev_SwitchBEEP	控制蜂鸣器
0x1C	dev_SwitchLED	控制 LED 灯
0x2E	dev_ReadNow	从命令超时等待立刻切换回正常读卡方式

ISO14443 协议		
0x40	iso14_RequestA	TypeA 寻卡
0x41	iso14_Anticoll	TypeA 防冲突
0x42	iso14_Select	TypeA 选定卡
0x43	iso14_ReqAntiSelect	TypeA 集寻卡，防冲突，选卡一体
0x44	iso14_HaltA	TypeA 卡休眠
0x45	iso14_RequestB	TypeB 寻卡
0x46	iso14_SlotMarker	TypeB 设置间隙
0x47	iso14_AttriB	TypeB 协商设置速率
0x48	iso14_HaltB	TypeB 卡休眠
0x49	iso14_RatsA	TypeA 获取卡片速率
0x4A	iso14_PpsRate	TypeA 协商设置速率
0x4B	iso14_APDU	ISO14443-4 APDU 通道
0x4C	card_GetSnr	获取卡片序列号。TypeA、TypeB、ID 卡、iso15693、felica
Mifare 卡操作		
0x50	mf_AuthKey	Mifare 卡验证密码
0x51	mf_Read	Mifare 卡读块
0x52	mf_Write	Mifare 卡写块
0x54	mf_OSRead	Mifare 卡操作集合寻卡、反冲突、选卡、验证密码、读块
0x55	mf_OSWrite	Mifare 卡操作集合寻卡、反冲突、选卡、验证密码、写块
0x56	mf_OSInitValue	Mifare 卡操作集合寻卡、反冲突、选卡、验证密码、初始化钱包值
0x57	mf_OSDecrement	Mifare 卡操作集合寻卡、反冲突、选卡、验证密码、扣款
0x58	mf_OSIncrement	Mifare 卡操作集合寻卡、反冲突、选卡、验证密码、充值
0x59	mf_OSGetValue	Mifare 卡操作集合寻卡、反冲突、选卡、验证密码、获取钱包值

125KHz 低频卡操作		
0x5A	lf_ReadBlock	T5577 卡读块
0x5B	lf_WriteBlock	T5577 卡写块
0x5C	lf_FormatIDnum	T5577 卡格式化成 ID 卡
0x5D	lf_AnthReadBlock	T5577 卡验证密码读块
0x5E	lf_AnthWriteBlock	T5577 卡验证密码写块

3.3 命令返回状态列表

状态列表		
状态码	**名称**	**描述**
0x00	ret_Ok	命令执行成功
0x01	ret_Fail	命令操作失败（具体说明参见函数）
0x31	ret_MonitorData	主动上传的数据
0x80	ret_NoSupportCmd	不支持此命令
0x81	ret_LenghtErr	数据长度错误
0x82	ret_AuthErr	验证失败
0x83	ret_TimeOut	处理超时
0x84	ret_NoCard	无卡响应
0x85	ret_ParamErr	传入参数不正确
0x86	ret_CmdCheckErr	命令校验错误
0x87	ret_UndefErr	未定义错误
0x88	ret_NoEnoughSpace	没有足够的空间

4 命令详细分析

4.1 dev_GetInfo (0x0B)：读取设备信息

- **命令描述：**

可读取出设备的部分信息，

- **发送数据：** N/A
- **正确返回：**

STATUS： 0x00-OK

数据包含设备名称、硬件版本、芯片序列号、固件编译日期

- **错误返回：**

STATUS： 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 01 0B 0A BA

返回数据包：AB 02 00 00 53 00 44 45 56 5F 4E 41 4D 45 3A 47 36 20 48 57 3A 30 33 34 31 20 0D 0A 53 4E 3A 31 43 43 30 30 32 30 39 42 44 35 32 36 30 30 34 30 30 33 32 34 44 34 44 0D 0A 42 75 69 6C 64 20 54 69 6D 65 3A 4E 6F 76 20 31 38 20 32 30 32 30 20 31 37 3A 31 37 3A 34 31 1B BA

DEV_NAME:G6 HW:0341

SN:1CC00209BD52600400324D4D

Build Time:Nov 18 2020 17:17:41

4.2 dev_UpFirmware (0x0C)：更新固件

- **命令描述：**

对设备固件进行更新升级，进入 IAP 模式之后才能使用。**更新固件模式下，波特率固定为 115200**。固件分包最大 1024 字节一包。

- **发送数据：**

DATA[0-1]： 固件一共多少包。

DATA[2-3]： 当前是第几包。从 0 包开始。

DATA[4-N]： 一包最大 1024 字节。最后一包按实际大小。

- **正确返回：**

STATUS： 0x00-OK

最后一包成功会返回 4 字节的 CRC 校验结果。

- **错误返回：**

STATUS： 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：

返回数据包：

4.3 dev_EnterIAP (0x0E)：进入 IAP 模式

- **命令描述：**

该命令使正常工作状态的设备重启进入升级模式。

- **发送数据：** N/A
- **正确返回：**

STATUS： 0x00-OK
模块进入升级模式的之后蜂鸣器会快速嘀嘀嘀几次，灯也会快速闪烁几次。

- **错误返回：**

STATUS： 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 01 0E 0F BA
返回数据包：AB 02 00 00 01 00 03 BA

4.4 dev_ExitIAP (0x0F)：退出 IAP 模式

- **命令描述：**

该命令使升级模式下的设备重启进入正常工作模式，如果没有升级固件成功，或者没有固件，则可能会导致设备无法再使用。

- **发送数据：** N/A
- **正确返回：**

STATUS： 0x00-OK
模块进入升级模式的时候蜂鸣器会快速嘀嘀嘀几次，灯也会快速闪烁几次。

- **错误返回：**

STATUS： 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 01 0F 0E BA
返回数据包：AB 01 00 00 01 00 00 BA

4.5 dev_SetBaud(0x10)：设置设备通信速率

- **命令描述：**

该命令用于设置设备和主机的通信波特率，重启模块生效。支持 TTL、RS232、RS485 进行设置。

- **发送数据：**

DATA[0]: 通信波特率
0x00-115200bps(默认)
0x01-57600bps
0x02-38400bps
0x03-19200bps
0x04-9600bps

- **正确返回：**

STATUS： 0x00-OK

- **错误返回：**

STATUS： 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 02 10 01 13 BA(设置波特率为 57600,N,8,1)
返回数据包：AB 01 00 00 01 00 00 BA

4.6 dev_SetAddr(0x11)：设置设备地址

- **命令描述：**

该命令用于设置模块的通信地址，可不用设置，默认为 0x00。该模式立即生效，重启依然有效。模块不过滤 0x00 和 0xFF 地址。

- **发送数据：**

DATA[0]: 模块地址

- **正确返回：**

STATUS: 0x00-OK
DATA[0]: 当前设备地址

- **错误返回：**

STATUS: 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 02 11 01 12 BA(设置的设备地址为 0x01)
返回数据包：AB 01 01 00 01 00 01 BA

4.7 dev_SetWorkMode(0x16)

- **命令描述：**

该命令可切换设备的工作模式。该模式立即生效，重启依然有效。

- **发送数据：**

DATA[0]: 设备工作模式
0x00-主动上传模式(默认)
0x01-命令通信模式

- **正确返回：**

STATUS: 0x00-OK

- **错误返回：**

STATUS: 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 02 16 01 15 BA （仅使用命令通信）
返回数据包：AB 01 00 00 01 00 00 BA

4.8 dev_Restart(0x17)

- **命令描述：**

该命令可让设备立即重启。

- **发送数据：** N/A

- **正确返回：**

STATUS: 0x00-OK

- **错误返回：**

STATUS: 错误代码，详细请看状态列表。
返回命令之后，延迟 100ms 设备立即重启。

- **通信例子：**

发送数据包：AB 00 00 00 01 17 16 BA
返回数据包：AB 00 00 00 01 00 01 BA

4.9 dev_SwitchRF(0x1A)

- **命令描述：**

该命令单独设置高低频射频信号的开和关，只在命令模式有效，重启恢复。

- **发送数据：**

DATA[0]: 0x01-HF 高频 13.56MHz
DATA[1]: 0x00-开
0x01-关

- **正确返回：**

STATUS: 0x00-OK
DATA[0]: 射频信号当前状态
0x00-开
0x01-关

- **错误返回：**

STATUS: 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 02 1A 00 18 BA
返回数据包：AB 01 00 00 02 00 00 03 BA

4.10 dev_SwitchBEEP(0x1B)

- **命令描述：**

该命令单独设置蜂鸣器响灭的时间和频率

- **发送数据：**

DATA[0]: 响的时间。单位为 10ms，1-255。可以只有这一个参数。
DATA[1]: 灭的时间。单位为 10ms，0-255。
DATA[2]: 响几次。1-20,最大 20 次

- **正确返回：**

STATUS: 0x00-OK

- **错误返回：**

STATUS: 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 02 1B 14 0D BA (响 200ms)
返回数据包：AB 01 00 01 00 00 BA

发送数据包：AB 00 00 00 04 1B 14 14 02 1D BA (响 200ms 灭 200ms 两次)
返回数据包：AB 01 00 01 00 00 BA

4.11 dev_SwitchLED(0x1C)

- **命令描述：**

该命令单独设置 LED 灯亮灭的时间和频率

- **发送数据：**

DATA[0]: 亮的时间。单位为 10ms，1-255。可以只有这一个参数。
DATA[1]: 灭的时间。单位为 10ms，0-255。
DATA[2]: 亮几次。1-255
DATA[3]: 操作几个灯。（该参数可不发送）

DATA[4-N]: 灯号。（该参数根据 DATA[3]发送）

- **正确返回：**

STATUS: 0x00-OK

- **错误返回：**

STATUS: 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 02 1C 32 2C BA （灯闪 500ms）

返回数据包：AB 00 00 00 01 00 01 BA

4.12 dev_ReadNow(0x2E)

- **命令描述：**

从命令超时等待立刻切换会正常读卡方式。此命令可用于主动读卡模式下，又需要命令通信读扇区，发送命令之后不需要 3 秒超时等待切换到主动读卡模式。

- **发送数据：** N/A
- **正确返回：**

STATUS: 0x00-OK

- **错误返回：**

STATUS: 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 01 2E 2F BA

返回数据包：AB 02 00 00 01 00 03 BA

4.13 iso14_RequestA(0x40)

- **命令描述：**

ISO14443A 协议中的寻卡指令。

- **发送数据：**

DATA[0]: 0x26-寻找没在休眠状态的卡片
0x52-寻找所有卡片

- **正确返回：**

STATUS: 0x00-OK

DATA[0-1]: 卡片请求应答 ATQA

- **错误返回：**

STATUS: 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 02 40 26 64 BA

返回数据包：AB 00 00 00 03 00 04 00 07 BA

4.14 iso14_Anticoll(0x41)

- **命令描述：**

ISO14443A 协议中的防冲突指令。

- **发送数据：**

DATA[0]: 0x93-一级防冲突代码
0x95-二级防冲突代码
0x97-三级防冲突代码

- **正确返回：**

STATUS： 0x00-OK
DATA[0-3]： 4 字节卡片序列号

- **错误返回：**

STATUS： 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 02 41 93 D0 BA
返回数据包：AB 00 00 00 05 00 A6 10 68 C2 19 BA

4.15 iso14_Select(0x42)

- **命令描述：**

ISO14443A 协议中的选定卡片指令。

- **发送数据：**

DATA[0]： 0x93-一级防冲突代码
0x95-二级防冲突代码
0x97-三级防冲突代码
DATA[1-5]： 防冲突指令中返回的卡片序列号

- **正确返回：**

STATUS： 0x00-OK
DATA[0]： 卡片选择应答 SAK

- **错误返回：**

STATUS： 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 06 42 93 A6 10 68 C2 CB BA
返回数据包：AB 00 00 00 02 00 08 0A BA

4.16 iso14_ReqAntiSelect(0x43)

- **命令描述：**

集合 ISO14443A 寻卡、防冲突、选卡操作，一条命令即可获取卡号。

- **发送数据：**

DATA[0]： 寻卡模式
0x26-IDEL 模块
0x52-ALL 模式

- **正确返回：**

STATUS： 0x00-OK
DATA[0-1]： 卡片 ATQA
DATA[2]： 卡片应答 SAK
DATA[3]： 卡号长度
DATA[4-N]： 卡号

- **错误返回：**

STATUS： 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 02 43 26 67 BB
返回数据包：AB 00 00 00 09 00 04 00 08 04 A6 10 68 C2 1D BA

4.17 iso14_HaltA(0x44)

- **命令描述：**

该命令用于使卡片进入休眠状态，卡片工作在 ISO14443-4 层 CPU 卡状态的情况下不能使用。

- **发送数据：** N/A
- **正确返回：**

STATUS： 0x00-OK

- **错误返回：**

STATUS： 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 01 44 45 BA

返回数据包：AB 00 00 00 01 00 01 BA

4.18 iso14_RequestB(0x45)

- **命令描述：**

ISO14443B 协议中的寻卡指令。

- **发送数据：**

DATA[0]: 0x00-空闲的卡
0x08-所有的卡

DATA[1]: AFI 应用标识符，默认 0x00 全选

DATA[2]: 时隙总数 N（0-1N，1-2N，2-4N，3-8N，4-16N）

- **正确返回：**

STATUS： 0x00-OK

DATA[0-11]: 卡片请求应答 ATQB

- **错误返回：**

STATUS： 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 04 45 08 00 00 49 BA

返回数据包：AB 02 00 00 0D 00 50 00 00 00 00 D1 03 00 81 00 70 C0 BC BA
(PUPI 为：00 00 00 00)

4.19 iso14_SlotMarker(0x46)

- **命令描述：**

该命令用于选择时隙。

- **发送数据：**

DATA[0]: 时隙总数 N（0-1N，1-2N，2-4N，3-8N，4-16N）

- **正确返回：**

STATUS： 0x00-OK

- **错误返回：**

STATUS： 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 02 46 00 44 BA（0-1N）

返回数据包：AB 00 00 00 01 00 01 BA

4.20 iso14_AttriB(0x47)

- **命令描述：**

ISO14443B 协议卡片协商通信速率。

- **发送数据：**

DATA[0-3]: 4 字节 PUPI
DATA[4]: BIT1(EOF:0-开启，1-关闭) BIT0(SOF:0-开启，1-关闭)
DATA[5]: PCD<-->PICC 速率选择
BIT3-BIT2(PICC->PCD:0-106K、1-212K、2-424K、3-848K)
BIT1-BIT0(PCD->PICC:0-106K、1-212K、2-424K、3-848K)
DATA[6]: CID

- **正确返回：**

STATUS： 0x00-OK

- **错误返回：**

STATUS： 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 08 47 00 00 00 00 00 00 00 4F BA
返回数据包：AB 00 00 00 01 00 01 BA

4.21 iso14_HaltB(0x48)

- **命令描述：**

ISO14443B 协议卡片进入休眠。

- **发送数据：**

DATA[0-3]: 4 字节 PUPI

- **正确返回：**

STATUS： 0x00-OK

- **错误返回：**

STATUS： 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 05 48 00 00 00 00 4D BA
返回数据包：AB 00 00 00 01 00 01 BA

4.22 iso14_RatsA(0x49)

- **命令描述：**

该命令为 ISO14443A 中 RatsA 指令，主要用于支持 ISO14443-4 协议的卡片复位。选择卡片之后才能使用该命令。

- **发送数据：**

DATA[0]: CID

- **正确返回：**

STATUS： 0x00-OK
DATA[0-N]: 卡片 ATS 应答的数据。

- **错误返回：**

STATUS： 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 02 49 01 4A BA
返回数据包：AB 00 00 00 11 00 10 78 80 A0 02 20 90 00 00 00 00 00 93 43 7A 0A 4B BA

4.23 iso14_PpsRate(0x4A)

- **命令描述：**

ISO14443A 协议卡片协商通信速率，需要卡片返回的 ATS 支持才行。

- **发送数据：**

DATA[0]: PCD<-->PICC 速率选择
BIT3-BIT2(PICC->PCD:0-106K、1-212K、2-424K、3-848K)
BIT1-BIT0(PCD->PICC:0-106K、1-212K、2-424K、3-848K)

- **正确返回：**

STATUS: 0x00-OK

- **错误返回：**

STATUS: 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 02 4A 0A 42 BA(设置通信速率为 424K)
返回数据包：AB 00 00 00 01 00 01 BA

4.24 iso14_APDU(0x4B)

- **命令描述：**

该命令用于支持 ISO14443-4 协议的卡片。复位卡片之后才能正确使用该命令。

- **发送数据：**

DATA[0]: CLA
DATA[1]: INS
DATA[2]: P1
DATA[3]: P2
DATA[4]: Lc
DATA[5-N]: Data（如果 Lc 为 0，则没有数据需要发送）
DATA[N+1]: Le（如果没有则不发送）

- **正确返回：**

STATUS: 0x00-OK
DATA[0-N]: 卡片返回的数据。

- **错误返回：**

STATUS: 0x01-FAIL
DATA[0]: 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 08 4B 00 A4 00 00 02 3F 00 DA BA(目录 MF 3F00)
返回数据包：AB 00 00 00 1A 00 6F 15 84 0E 31 50 41 59 2E 53 59 53 2E 44 44 46 30 31 A5 03 88 01 01 90 00 33 BA

4.25 card_GetSnr(0x4C)

- **命令描述：**

通过设备获取当前卡片序列号，轮询所有设备支持的卡片协议。比较耗时的命令

- **发送数据：** N/A

- **正确返回：**

STATUS: 0x00-OK

DATA[0]: 卡片类型
DATA[1]: 卡号长度
DATA[2-N]: 卡号

- **错误返回:**

STATUS: 错误代码，详细请看状态列表。

- **通信例子:**

发送数据包：AB 00 00 00 01 4C 4D BA
返回数据包：AB 02 00 00 07 00 10 04 AB CC 06 B3 C3 BA

4.26 mf_AuthKey(0x50)

- **命令描述:**

Mifare 卡片密钥验证。

- **发送数据:**

DATA[0]: 0x60-A 组密钥
0x61-B 组密钥
DATA[1]: 指定块 S50 最大 63 块，S70 最大 255 块
DATA[2-7]: 6 字节密钥，默认全为 FF
DATA[8-11]; 4 字节卡片序列号

- **正确返回:**

STATUS: 0x00-OK

- **错误返回:**

STATUS: 错误代码，详细请看状态列表。

- **通信例子:**

发送数据包：AB 00 00 00 0D 50 60 04 FF FF FF FF FF FF A6 10 68 C2 25 BA
返回数据包：AB 00 00 00 01 00 01 BA

4.27 mf_Read(0x51)

- **命令描述:**

Mifare 卡片读指定块,一块 16 字节。

- **发送数据:**

DATA[0]: 指定块 S50 最大 63 块，S70 最大 255 块

- **正确返回:**

STATUS: 0x00-OK
DATA[0-15]: 16 字节块数据。

- **错误返回:**

STATUS: 错误代码，详细请看状态列表。

- **通信例子:**

发送数据包：AB 00 00 00 02 51 04 57 BA
返回数据包：AB 00 00 00 11 00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 11 BA

4.28 mf_Write(0x52)

- **命令描述:**

Mifare 卡片写指定块,一块 16 字节。

- **发送数据:**

DATA[0]: 指定块 S50 最大 63 块，S70 最大 255 块

DATA[1-16]: 块数据

- **正确返回:**

STATUS: 0x00-OK

- **错误返回:**

STATUS: 错误代码，详细请看状态列表。

- **通信例子:**

发送数据包：AB 00 00 00 12 52 04 31 32 33 34 35 36 37 38 31 32 33 34 35 36 37 38 44 BA（块 4）

返回数据包：AB 00 00 00 01 00 01 BA

4.29 mf_OSRead(0x54)

- **命令描述:**

Mifare 跨扇区读，跳过密钥块不读，必须每个扇区密钥一样才能成功。
此命令自动寻卡、防冲突、选卡，然后根据密钥验证扇区读出数据。

- **发送数据:**

DATA[0]: 0x60-A 组密钥
0x61-B 组密钥

DATA[1]: 开始要读的块

DATA[2]: 一共要读的块，不包括密钥块

DATA[3-8]: 密钥

- **正确返回:**

STATUS: 0x00-OK

DATA[0-N]: 16 倍数的块数据。

- **错误返回:**

STATUS: 错误代码，详细请看状态列表。

- **通信例子:**

发送数据包：AB 00 00 00 0A 54 60 04 05 FF FF FF FF FF FF 3F BA(从第 0x04 块开始读 5 块，跨扇区了，但是不读扇区的密钥块)

返回数据包：AB 00 00 00 51 00 31 32 33 34 35 36 37 38 31 32 33 34 35 36 37 38 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 51 BA

4.30 mf_OSWrite(0x55)

- **命令描述:**

Mifare 跨扇区写，跳过密钥块不写，必须每个扇区密钥一样才能成功。
此命令自动寻卡、防冲突、选卡，然后根据密钥验证扇区写入数据。

- **发送数据:**

DATA[0]: 0x60-A 组密钥
0x61-B 组密钥

DATA[1]: 从哪一块开始写

DATA[2-7]: 密钥

DATA[8-n]: 写入数据，16 个字节为一个单位，写完一块，自动切换写下一块，跳过密钥块不写。

- **正确返回：**

STATUS： 0x00-OK

- **错误返回：**

STATUS： 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 39 55 60 04 FF FF FF FF FF FF 31 32 33 34 35 36 37 38 31 32 33 34 35 36 37 38 31 32 33 34 35 36 37 38 31 32 33 34 35 36 37 38 31 32 33 34 35 36 37 38 08 BA

返回数据包：AB 00 00 00 01 00 01 BA

4.31 mf_OSInitValue(0x56)

- **命令描述：**

Mifare 卡使用钱包功能，随便指定一块作为钱包功能。

此命令自动寻卡、防冲突、选卡，然后根据密钥验证初始化钱包值。

- **发送数据：**

DATA[0]: 0x60-A 组密钥

0x61-B 组密钥

DATA[1]: 使用哪一块作为钱包功能

DATA[2-7]: 密钥

DATA[8-11]: int 类型的钱包值（大端模式）

- **正确返回：**

STATUS： 0x00-OK

- **错误返回：**

STATUS： 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 0D 56 60 04 FF FF FF FF FF FF 00 00 03 E8 D4 BA(钱包值为 1000)

返回数据包：AB 00 00 00 01 00 01 BA

4.32 mf_OSDecrement(0x57)

- **命令描述：**

Mifare 卡使用钱包功能，对指定块中的钱包扣款。

此命令自动寻卡、防冲突、选卡，然后根据密钥验证扣款。

- **发送数据：**

DATA[0]: 0x60-A 组密钥

0x61-B 组密钥

DATA[1]: 哪一块为钱包值

DATA[2-7]: 密钥

DATA[8-11]: int 类型的值（大端模式）

- **正确返回：**

STATUS： 0x00-OK

- **错误返回：**

STATUS： 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 0D 57 60 04 FF FF FF FF FF FF 00 00 03 E8 D5 BA(扣款值为 1000)

返回数据包：AB 00 00 00 01 00 01 BA

4.33 mf_OSIncrement(0x58)

- **命令描述：**

Mifare 卡使用钱包功能，对指定块中的钱包充值。

此命令自动寻卡、防冲突、选卡，然后根据密钥验证充值。

- **发送数据：**

DATA[0]: 0x60-A 组密钥
0x61-B 组密钥

DATA[1]: 哪一块为钱包值

DATA[2-7]: 密钥

DATA[8-11]: int 类型的值（大端模式）

- **正确返回：**

STATUS: 0x00-OK

- **错误返回：**

STATUS: 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 0D 58 60 04 FF FF FF FF FF FF 00 00 03 E8 DA BA(充值值为 1000)

返回数据包：AB 00 00 00 01 00 01 BA

4.34 mf_OSGetValue (0x59)

- **命令描述：**

Mifare 卡使用钱包功能，随便指定一块作为钱包功能。

此命令自动寻卡、防冲突、选卡，然后根据密钥验证初始化钱包值。

- **发送数据：**

DATA[0]: 0x60-A 组密钥
0x61-B 组密钥

DATA[1]: 使用哪一块作为钱包功能

DATA[2-7]: 密钥

- **正确返回：**

STATUS: 0x00-OK

DATA[0-3]: 4 字节钱包值（大端模式）。

- **错误返回：**

STATUS: 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 09 59 60 04 FF FF FF FF FF FF 34 BA

返回数据包：AB 00 00 00 05 00 00 00 03 E8 EE BA

4.35 lf_ReadBlock(0x5A)

- **命令描述：**

T5577 卡读某一块数据，使用曼彻斯特编码。

- **发送数据：**

DATA[0]: 速率。16、32、40、50、64、100、128
DATA[1]: 哪一页。0、1
DATA[2]: 哪一块。0、1、2、3、4、5、6、7

- **正确返回：**

STATUS: 0x00-OK

- **错误返回：**

STATUS: 错误代码，详细请看状态列表。
DATA[0-3]: 4 字节块数据。

- **通信例子：**

发送数据包：AB 00 00 00 04 5A 40 00 00 1E BA (速度 64，page0 block0)
返回数据包：AB 02 00 00 05 00 00 14 80 41 D2 BA

4.36 lf_WriteBlock(0x5B)

- **命令描述：**

T5577 卡写某一块数据，使用曼彻斯特编码。

- **发送数据：**

DATA[0]: 哪一页。0、1
DATA[1]: 哪一块。0、1、2、3、4、5、6、7
DATA[2]: 是否锁住。0-不锁，1-锁住
DATA[3-4]: 4 字节块数据

- **正确返回：**

STATUS: 0x00-OK

- **错误返回：**

STATUS: 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 08 5B 00 01 00 31 32 33 34 56 BA
返回数据包：AB 02 00 00 01 00 03 BA

4.37 lf_FormatIDnum(0x5C)

- **命令描述：**

把 T5577 卡格式化成 ID 卡。

- **发送数据：**

DATA[0-4]: 5 字节 ID 卡号，第一个字节一般不使用
DATA[5]: 是否锁卡。0-不锁卡，1-锁卡

- **正确返回：**

STATUS: 0x00-OK

- **错误返回：**

STATUS: 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 07 5C 2E 00 6F 85 B6 00 29 BA
返回数据包：AB 02 00 00 01 00 03 BA

4.38 lf_AnthReadBlock(0x5D)

- **命令描述：**

T5577 卡验证密码读某一块数据，使用曼彻斯特编码。

- **发送数据：**

DATA[0]: 速率。16、32、40、50、64、100、128
DATA[1]: 哪一页。0、1
DATA[2]: 哪一块。0、1、2、3、4、5、6、7
DATA[3-6]: 4 个字节密码。密码存在块 7.

- **正确返回：**

STATUS: 0x00-OK

- **错误返回：**

STATUS: 错误代码，详细请看状态列表。
DATA[0-3]: 4 字节块数据。

- **通信例子：**

发送数据包：AB 00 00 00 08 5D 40 00 01 FF FF FF FF 14 BA (速度 64，page0 block1 密码 FF FF FF FF)
返回数据包：AB 02 00 00 05 00 30 31 32 33 07 BA

4.39 lf_AnthWriteBlock(0x5E)

- **命令描述：**

T5577 卡验证密码写某一块数据，使用曼彻斯特编码。

- **发送数据：**

DATA[0]: 哪一页。0、1
DATA[1]: 哪一块。0、1、2、3、4、5、6、7
DATA[2]: 是否锁住。0-不锁，1-锁住
DATA[3-4]: 4 字节密码
DATA[5-8]: 4 字节块数据

- **正确返回：**

STATUS: 0x00-OK

- **错误返回：**

STATUS: 错误代码，详细请看状态列表。

- **通信例子：**

发送数据包：AB 00 00 00 0C 5E 00 01 00 FF FF FF FF 31 32 33 34 57 BA
返回数据包：AB 02 00 00 01 00 03 BA

5 主动上传卡号模式说明

5.1 数据包格式

不同型号产品可能略有差异，请以产品说明书为准。

数据头	长度	卡片类型	卡号数据	异或校验	数据尾
0x02	包含数据头尾	参考附录一	4-8 字节	不包含数据头尾	0x03

5.2 举例说明

例如：串口工具接收到的数据为 02 0A 01 2E 00 B6 D7 B5 F1 03

第一个字节 0x02 表示数据开始。

第二个字节 0x0A 表示整条数据长度为 10 个字节，包括数据开始和数据结束。

第三个字节 0x01 表示该卡片类型为 EM4100。

第四个字节到第八个字节(0x2E 0x00 0xB6 0xD7 0xB5)这 5 个字节 表示读取到的卡号，其中第四个字节 0x2E 为 ID 卡隐藏卡号。

第九个字节 0xF1 表示第二个字节到第八个字节的 BCC 校验。

第十个字节 0x03 表示数据结束。

6 注意事项

6.1 设备工作模式

6.1.1 监控上传模式（默认）

在此模式下，设备会主动上传数据到主机，并附带数据类型。

在此模式下，设备只响应设置工作模式命令和获取序列号命令。

编号	数据类型说明
0	未定义
1	卡号
2	二维码数据
3	触摸按键键值
4	实体按键（防盗开关）
5	软复位
6	其他

6.1.2 命令通信模式

此模式下，设备支持的命令需要参考设备的详细说明书。通信命令可查看 3.2 中的命令列表。

6.2 设备通信注意事项

6.2.1 关于设备类型

设备类型为 0 的时候，不管当前设备是什么类型，都可以响应命令，否则只响应符合自身设备类型的命令。

设备类型	说明
0	不过滤当前通信命令
1	模块
2	读卡器
3	发卡器
4	主板
5	控制器
6	其他

6.2.2 关于设备地址

设备地址为 0x00 或者 0xFF 的时候，不管当前设备是什么地址，一定会响应命令，否则只响应符合自身地址的命令。

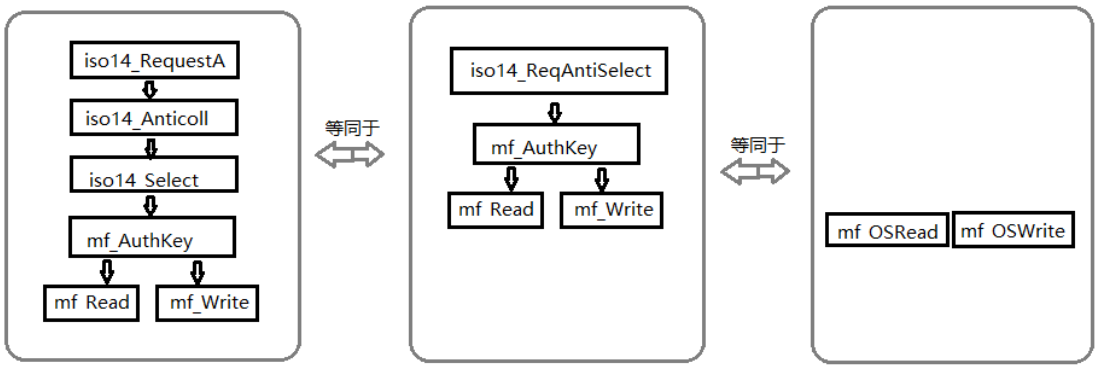
7 附录

7.1 附录一、卡片类型

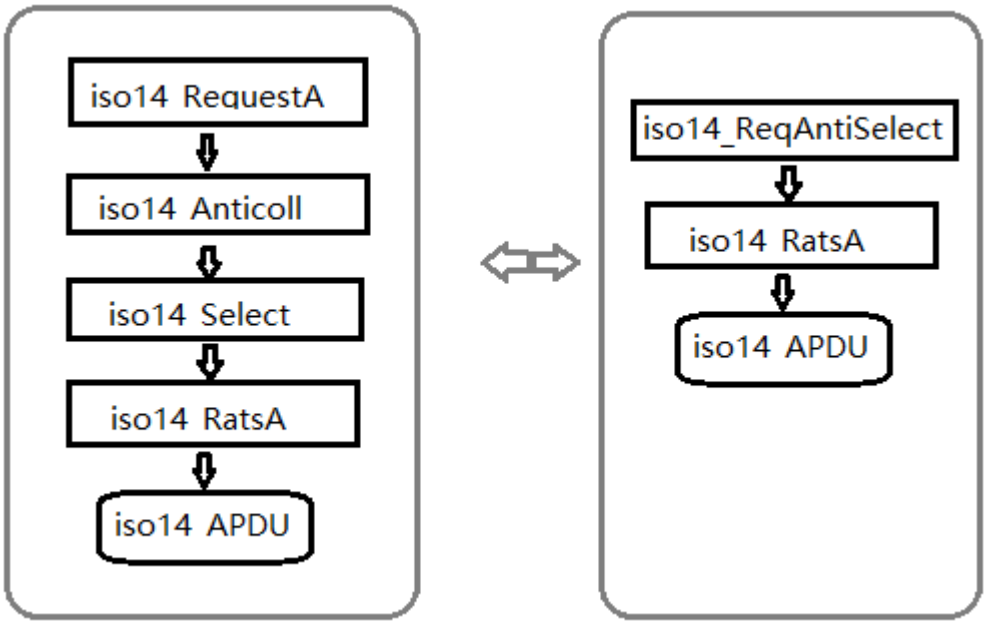
卡片类型			
编码	**卡片名称**	**卡号长度**	**备注**
0x01	EM41XX	5	ID 卡
0x02	T5577	4	
0x03	HID Prox	8	
0x10	TypeA-4Byte	4	Mifare1K/S50/S70
0x11	TypeA-7Byte	7	
0x12	TypeA-10Byte		
0x13	PBOC	8	银行卡、手机 PAY，把 17 或者 19 位十进制银行卡号转为 8 字节十六进制
0x14	DesFire(加密信息)	7	DesFire 中文件内容
0x15	FMcos(加密信息)	4	CPU 卡中文件内容
0x16	Gicard	4	深圳市长城物联科技有限公司-G 卡
0x17	MifareBlock	16	Mifare 卡块数据
0x18	MFOEM1	不定长	CPU 卡定制
0x19	TypeA-CPU	4	TypeA 协议的 CPU 卡 uid 号
0x20	ChinaID	8	二代证 uid 号
0x21	TypeB-4Byte	4	
0x30	Felica	8	索尼卡
0x31	15693-8Byte	8	标签卡
0x32	iClass	8	
0xFF	Keyboard	1	按键类型

（注：此表格中卡片类型为自定义，仅供参考，各个型号产品略有不同。）

7.2 附录二、Mifare 卡操作流程



7.3 附录三、CPU 卡操作流程



注：APDU 命令用于和 CPU 卡通信，例如获取随机数、选中文件、外部认证、读二进制文件

8 联系方式

深圳市长城物联科技有限公司
地址：深圳市龙华新区观湖街道樟坑径下围工业区景山大厦 A 座 4G,4H.
电话：0755-28579196
邮箱：master@gwiot.com