

HS520A 模块使用说明

Ver 1.00

深圳华视电子读写设备有限公司

1. 适用范围

HS520A 读写模块，适用于 ISO14443A 协议下的各种应用。目前该版本只支持 S50，S70 等各种 Mifare1 卡片的读写。

2. HS520A 模块简介

HS520A 是一个简单的串行读写模块，接口为 CMOS 电平，用于与常用的微处理器（如单片机、ARM）的 UART 接口；当外接 RS232 电平转换电路，能够与 PC 机的串口连接通信。

用户必须通过主机（包括单片机、ARM、DSP 以及 PC 机等）向 HS520A 模块发送命令来对 HS520A 进行读写控制。本应用指南将重点描述 HS520A 与主机之间的串行通信协议和命令。

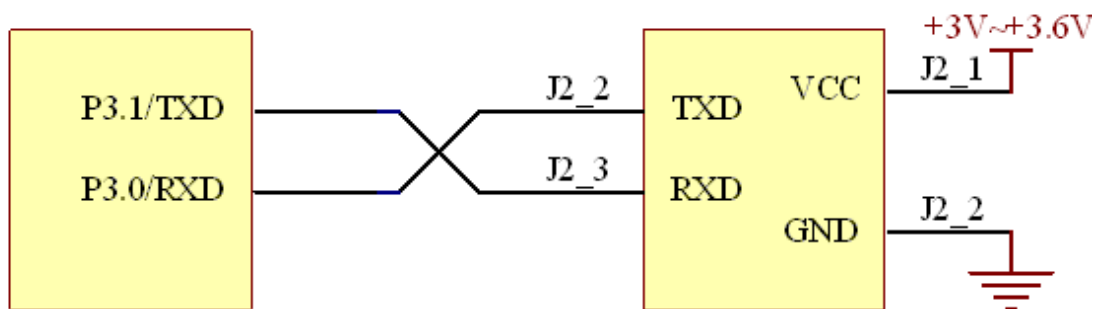
2.1 引脚描述

表1. HS520A的接口

符号	I/O 类型	功能描述	上电后的状态
GND(方形焊盘)	power	地	低
POWER	power	电源正极	高
MCU_TXD	输入	模块 URAT 的输入	高
MCU_RXD	输出	模块 URAT 的输出	高
WK_UP	输入	唤醒休眠状态下的模块	高
TAG	输出	有卡信号的输出：当在天线范围内寻到卡时，TAG 输出 300ms 负脉冲。	高

2.2 典型电路

HS520A 模块可以与任何带有 UART 口的 MCU 相连接，图 1 所示为 HS520A 与 MCS51 单片机 UART 的典型接口。



2.3 技术参数

表2. HS520A 模块技术参数表

产品型号	HS520 系列
功耗（直流 3.3V）	模块休眠电流：<2mA 模块待机电流：<20mA， 模块读卡电流：<70mA
工作频率	13.56MHz
读卡距离	30~60毫米（mifare1卡）
接口方式	UART
数据传输速率	UART：9600~115200bps
支持卡类型	mifare1 S50、mifare1 S70等各种符合 ISO14443A协议的逻辑加密卡以及CPU卡
尺寸：分体式(mm)	主板：20*49*3.15 天线板：30*50

3. HS520A 读卡模块数据传输协议

3.1. 串口协议

主机与 HS520A 串行接口通信过程中一帧的数据格式采用 1 个起始位，8 个数据位、无奇偶校验位、1 个停止位。通信协议分为两步，第一步波特率设置，第二步进行数据通信。用户可以通过串口调试助手来调试开发 HS520A，具体见 5 使用串口调试助手开发调试该模块。

3.2 控制字符定义

下表列出了 HS520A与主机串行通信过程中用到的控制字符定义。

表4. HS520A 串行通信控制字符表

描述	定义	值
开始符(主机-HS520A)	STX	0x0A
终止符(主机-HS520A)	ETX	0x0B
开始符(HS520A-主机)	STX	0x0C
终止符(HS520A-主机)	ETX	0x0D

3.3 协议描述

3.3.1 数据通信帧描述

数据通信以一帧为单位进行，格式如下：

表 5 数据通信帧结构

起始符 STX	包号 SEQNR	命令/状态 CMD/Status	数据长度 Length	数据 DATA	校验和 BCC	帧结束符 ETX
1byte	1byte	1byte	1byte	nbyte	1byte	1byte

数据帧中各字段说明如表 6 所示：

表6. 数据帧各字段说明

字段	长度	说明	补充
STX	1	主机—从机: TX=0x0A 从机—主机: TX=0x0C 数据帧的起始符, 每一帧数据都是以 STX 开始	
SEQNR	1	该数据帧包序号, 可以为 0 到 255 的任意值。可以用来作为通信间的错误检查, 从机(模块)接收到主机发来的信息, 在应答信息中发出一个同样的 SEQ信息, 主机可以通过此信息检查是否发生的“包丢失”的错误。第一个包的 SEQ 可为任意值。	该字段主机发送和接收的应该相同
Cmd/Status	1	主机—从机: 命令 Command 从机—主机: 状态 Status	
Length	1	该帧所带数据信息长度	
DATA	Length	数据信息, 长度等于 Length	
BCC	1	校验和。从帧头(STX)开始到数据(DATA)的最后一字节异或取反。	
ETX	1	主机—从机: TX=0x0B 从机—主机: TX=0x0D 是一个帧的结束标志	

数据帧接收规则:

- 1 一帧的结束一定是 ETX, 但接收到 0x0B 则不一定是帧结束;
- 1 帧长必须不小于 6 字节, 最大不能超过 64 字节。
- 1 BCC 计算必须正确。

3.3.2 主机发送命令至模块

通信必须先由主机发送命令和数据给 HS520A，HS520A执行命令完毕后，再将执行命令后的状态和响应数据发回给主机。用户在给 HS520A 模块发送命令时，连续的发送 STX (0x0A)+...+0x0B(结束符)。通过判断HS520A返回数据的正确性来判断HS520A是否正确执行了本条命令。

表8. 主机发送给HS520A遵循的格式

STX	SEQNR	CMD	Length	DATA	BCC	ETX
0x0A						0x0B

3.3.3 从机返回数据给主机

HS520A在接收到主机发送的数据后，根据数据块的内容执行相应命令，并将执行命令后的状态或者数据（以下将状态和数据都统称为数据）返回给主机。

表9. HS520A发送格式

STX	SEQNR	Status	Length	DATA	BCC	ETX
0x0C						0x0D

命令集总览

Command	Description
0xA1	设置串口波特率
0xA2	射频芯片启动的设置
0xA3	射频芯片休眠的设置
0xA4	读卡，防冲突，选卡
0xA5	认证密钥A/B
0xA6	写数据到块
0xA7	从块读数据
0xA8	卡休眠
0xA9	初始化块为电子钱包的格式
0xAA	电子钱包的操作（增值减值，值的传输）
0xAB	模块休眠的设置

状态总览

Status	Description
0x81	发送帧帧头错误
0x82	寻卡失败
0x83	防冲突失败
0x84	发送帧BCC错误
0x85	发送帧帧尾错误
0x86	认证失败
0x87	读卡失败
0x88	写卡失败
0x89	初始化失败
0x8A	电子钱包操作失败
0x8B	休眠失败
0x8C	发送帧CMD错误

命令集描述

1. 设置串口波特率（发送帧：主机-HS520A）

STX	SEQNR	CMD	Length	DATA	BCC	ETX
0x0A	自定义	0xA1	0x01	0x01-0x05	计算结果值	0x0B

DATA:

0x01: 9600bps
0x02: 19200bps
0x03: 38400bps
0x04: 57600bps
0x05: 115200bps

应答（接收帧：HS520A-主机）

STX	SEQNR	Status	Length	DATA	BCC	ETX
0x0C	同发送帧		0	/	计算结果值	0x0D

Status:

0x00: 操作成功
0x81: 发送帧帧头错误
0x84: 发送帧 BCC 错误
0x85: 发送帧帧尾错误
0x8C: 发送帧 CMD 错误

2. 射频芯片启动配置（发送帧：主机-HS520A）复位通信芯片并打开天线。

STX	SEQNR	CMD	Length	DATA	BCC	ETX
0x0A	自定义	0xA2	0	/	计算结果值	0x0B

应答（接收帧：HS520A-主机）

STX	SEQNR	Status	Length	DATA	BCC	ETX
0x0C	同发送帧		0	/	计算结果值	0x0D

Status:

- 0x00: 操作成功
- 0x81: 发送帧帧头错误
- 0x84: 发送帧 BCC 错误
- 0x85: 发送帧帧尾错误
- 0x8C: 发送帧 CMD 错误

3. 射频芯片休眠配置（发送帧：主机-HS520A）休眠通信芯片。

STX	SEQNR	CMD	Length	DATA	BCC	ETX
0x0A	自定义	0xA3	0	/	计算结果值	0x0B

应答（接收帧：HS520A-主机）

STX	SEQNR	Status	Length	DATA	BCC	ETX
0x0C	同发送帧		0	/	计算结果值	0x0D

Status:

- 0x00: 操作成功
- 0x81: 发送帧帧头错误
- 0x84: 发送帧 BCC 错误
- 0x85: 发送帧帧尾错误
- 0x8C: 发送帧 CMD 错误

4. 功能描述：读卡-防冲突-选卡（发送帧：主机-HS520A）

该命令为寻卡、防冲突和选卡三条命令的组合，寻找天线范围内的射频卡并返回卡类型代码（TagType），卡号（UID）以及 SAK 值，兼有防冲突的功能，并能寻 7 字节 UID 的卡。

成功执行该命令后即可进行验证及后续操作。

寻找的是天线范围内处于 IDLE 状态的卡（HALT 状态的除外）。

当天线范围内寻到卡时，LED1 灯闪烁 300ms。TAG 端输出 300ms 的负脉冲。

STX	SEQNR	CMD	Length	DATA	BCC	ETX
0x0A	自定义	0xA4	0	/	计算结果值	0x0B

应答（接收帧：HS520A-主机）

STX	SEQNR	Status	Length	DATA	BCC	ETX
0x0C	同发送帧			TagType, UID, SAK	计算结果值	0x0D

Status:

- 0x00: 操作成功
- 0x82: 寻卡失败
- 0x83: 防冲突失败

0x81: 发送帧帧头错误

0x84: 发送帧 BCC 错误

0x85: 发送帧帧尾错误

0x8C: 发送帧 CMD 错误

Length: 4 字节+序列号的长度

Mifare1 S50、S70、Light 卡: 8 字节

Mifare0 UltraLight 和 Mifare3 Desfire 卡: 11 字节

DATA[0..1]: *TagType: 请求应答, 2 个字节的卡片类型, 见表13, 14.

DATA[2]: *Sak: 最后一级选择应答的应答, 其意义见 ISO14443 带层级设置的防碰撞 -Casc_Anticoll, 见表15, 16.

DATA[3]: *SnrLen: 返回卡片序列号的长度

DATA[4..4+ SnrLen]: *Snr: 返回卡片的序列号

例如: 一张序列号为 0x007e0a42 的 Mifare1 S50 卡返回的数据

STX	SEQNR	Status	Length	DATA	BCC	ETX
0x0C	0x02	0x00	0x08	0x04 0x00 0x08 0x04 0x42 0x0A 0x7E 0x00	0xxx	0x0D

例如: 一张序列号为 0x000000007e0a42 的 Mifare UltraLight 卡返回的数据

STX	SEQNR	Status	Length	DATA	BCC	ETX
0x0C	0x02	0x00	0x0B	0x44 0x00 0x00 0x07 0x42 0x0A 0x7E 0x00 0x00 0x00 0x00	0xxx	0x0C

表 13 *TagType 的含义

Bit15-Bit8	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
保留	序列号大小 00:4bytes 01:7bytes 10:10bytes		保留	任何位为 1 时, 则为比特帧防碰撞方式				

各种常用卡返回的数据如下表 14 所示:

表 14 常用卡的TagType 值

卡类型	TagType	卡类型	TagType
Mifare1 S50	0x0004	SHC1101	0x0004
Mifare1 S70	0x0002	SHC1102	0x3300
Mifare Light	0x0010	11RF32	0x0004
Mifare UltraLight	0x0044		

表 15 *Sak 含义

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
RFU	RFU		RFU	RFU	判断是否 选择完成	RFU	RFU

Bit2 位用来判断是否还有序列号未读出，bit2=0 时，表示所有序列号输入完毕，选择成功，bit2=1 时表示序列号没有全部输入，选择没有完全成功，还要进行下一级的防碰撞和选择操作。

当*Sak=xxxx1xx 时，序列号没有完成，还要进行下一级的防碰撞和选择操作。

当*Sak=xx1xx0xx 时，选择成功，该卡符合 ISO/IEC 14443-4 标准。

当*Sak=xx0xx0xx 时，选择成功，该卡不符合 ISO/IEC 14443-4 标准。

各种常用卡返回的数据如下所表 16 所示：

表 16 常用卡的*Sak 的值

卡类型	Sak	卡类型	Sak
Mifare1 S50	0x08	Mifare0 UltraLight	0x04
Mifare1 S70	0x18	SHC1101	0x22
Mifare1 Light	0x01	11RF32	0x08

5. 认证密钥 A/B (发送帧：主机-HS520A) 对存储在卡片中的密钥 A/B 进行验证。

STX	SEQNR	CMD	Length	DATA	BCC	ETX
0x0A	自定义	0xA5	0x08	KEYA/B, Block, key	计算结果 值	0x0B

KEYA/B:

密钥类型 (1 字节)。可取值为 KeyAB=0x01 (KEYA)，利用密钥 A 进行验证，或 KeyAB=0x02 (KEYB)，利用密钥 B 进行验证。

Block: 所要验证的卡扇区号的相应块号 (即所要访问的扇区) (1 字节)。如扇区 1 为 4-7 块，若想对扇区 1 进行操作，就需要验证扇区 1，那么这里的块号为 4, 5, 6, 7 均可。

Key: 用于验证的密钥 (6 字节)。

应答（接收帧：HS520A-主机）

STX	SEQNR	Status	Length	DATA	BCC	ETX
0x0C	同发送帧		0	/	计算结果值	0x0D

Status:

- 0x00: 操作成功
- 0x86: 认证失败
- 0x81: 发送帧帧头错误
- 0x84: 发送帧 BCC 错误
- 0x85: 发送帧帧尾错误
- 0x8C: 发送帧 CMD 错误

6. 写数据到块 Write（发送帧：主机-HS520A）写 16 字节的数据到卡中相应的块。

STX	SEQNR	CMD	Length	DATA	BCC	ETX
0x0A	自定义	0xA6	0x11	Block, Data	计算结果值	0x0B

Block: 要写的块号。

Data: 16 个字节的数据。

应答（接收帧：HS520A-主机）

STX	SEQNR	Status	Length	DATA	BCC	ETX
0x0C	同发送帧		0	/	计算结果值	0x0D

Status:

- 0x00: 操作成功
- 0x88: 写失败
- 0x81: 发送帧帧头错误
- 0x84: 发送帧 BCC 错误
- 0x85: 发送帧帧尾错误
- 0x8C: 发送帧 CMD 错误

7. 从块读数据 Read（发送帧：主机-HS520A）读出存储在卡片中相应块的数据（16 个字节）。

STX	SEQNR	CMD	Length	DATA	BCC	ETX
0x0A	自定义	0xA7	0x01	Block	计算结果值	0x0B

Block: 所要读取的卡片的相应块的块号（1 字节）。

应答（接收帧：HS520A-主机）

STX	SEQNR	Status	Length	DATA	BCC	ETX
0x0C	同发送帧		0x10	Data	计算结果值	0x0D

Status:

- 0x00: 操作成功
- 0x87: 读失败
- 0x81: 发送帧帧头错误
- 0x84: 发送帧 BCC 错误
- 0x85: 发送帧帧尾错误
- 0x8C: 发送帧 CMD 错误

Data: 读取的数据 (16 个字节)。

8. 卡休眠Halt (发送帧: 主机-HS520A) 使卡片处于休眠状态, 处于此状态的卡片将不会对读卡-防冲突-选卡的操作产生响应。

STX	SEQNR	CMD	Length	DATA	BCC	ETX
0x0A	自定义	0xA8	0	/	计算结果值	0x0B

应答 (接收帧: HS520A-主机)

STX	SEQNR	Status	Length	DATA	BCC	ETX
0x0C	同发送帧		0x10	Data	计算结果值	0x0D

Status:

- 0x00: 操作成功
- 0x8B: 休眠失败
- 0x81: 发送帧帧头错误
- 0x84: 发送帧 BCC 错误
- 0x85: 发送帧帧尾错误
- 0x8C: 发送帧 CMD 错误

9. 初始化块为电子钱包的格式 (发送帧: 主机-HS520A)

使卡片块中存储的数据成为电子钱包的格式 (更详细的内容参考M1卡的介绍)。变成这种格式后, 可以对这种块进行电子钱包的操作 (增值, 减值, 复制)。

STX	SEQNR	CMD	Length	DATA	BCC	ETX
0x0A	自定义	0xA9	0x05	Block, Data	计算结果值	0x0B

Block: 所要初始化的卡片的相应块的块号 (1 字节)。

Data: 电子钱包的值 (4 字节)。

应答 (接收帧: HS520A-主机)

STX	SEQNR	Status	Length	DATA	BCC	ETX
0x0C	同发送帧		0	/	计算结果值	0x0D

Status:

- 0x00: 操作成功
- 0x89: 初始化失败
- 0x81: 发送帧帧头错误
- 0x84: 发送帧 BCC 错误
- 0x85: 发送帧帧尾错误
- 0x8C: 发送帧 CMD 错误

10. 电子钱包的操作（增值减值，值的传输）（发送帧：主机-HS520A）

对相应的块进行电子钱包的操作（增值，减值，值的传输）。

注意：值的传输只能在相同扇区的块之间进行，如果是相同的块，就是对一个块进行增减操作后写入原来的块，就是改变了该块的值。如果是不同的块，就是就是对一个块进行增减操作后放入其它的块。如果改变的值为0，就是单纯的复制了。

STX	SEQNR	CMD	Length	DATA	BCC	ETX
0x0A	自定义	0xAA	0x07	INDE, Block1, Data, Block2	计算结果值	0x0B

INDE: 操作方式（1 字节）。

0x01: 增值。

0x02: 减值。

Block1: 所要所要改写值的相应块的块号（1 字节）。

Data: 需要改变的值（4 字节）。

Block2: 改变后的值存放的块号。

应答（接收帧：HS520A-主机）

STX	SEQNR	Status	Length	DATA	BCC	ETX
0x0C	同发送帧		0	/	计算结果值	0x0D

Status:

- 0x00: 操作成功
- 0x8a: 电子钱包操作失败
- 0x81: 发送帧帧头错误
- 0x84: 发送帧 BCC 错误
- 0x85: 发送帧帧尾错误
- 0x8C: 发送帧 CMD 错误

11. 模块休眠配置（发送帧：主机-HS520A）休眠整个模块。

模块休眠后只能通过 WA_UP 引脚的低电平唤醒。唤醒后模块立即复位。

STX	SEQNR	CMD	Length	DATA	BCC	ETX
0x0A	自定义	0xab	0	/	计算结果值	0x0B

5. 使用串口调试助手开发调试 HS520A 模块

5.1 软硬件准备

1. HS520A模块一块，外接RS232转换
2. 串口电缆
3. 3.3V电源
4. 5根连线
5. Mifare卡一张
6. 串口调试软件
7. 串口监视软件（选）
8. PC机

5.2 设置串口调试软件

按照图 2 所示设置串口调试软件。

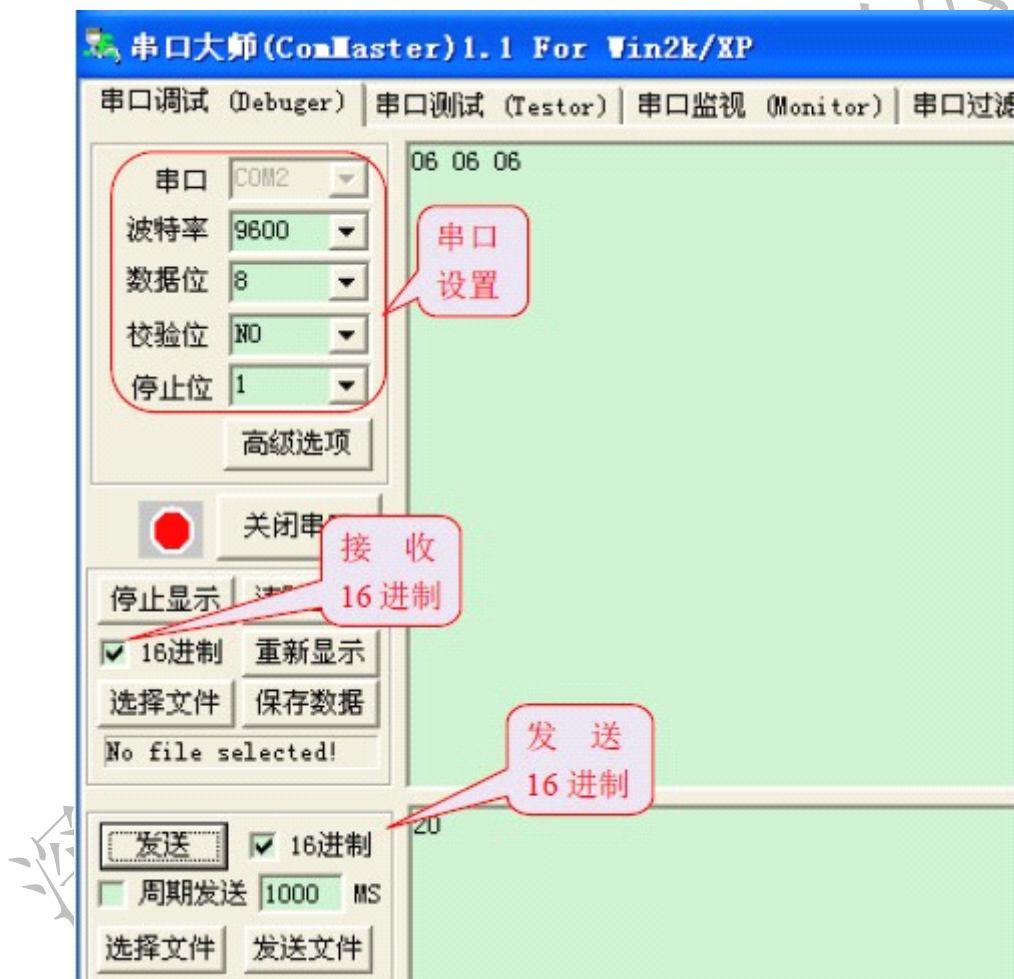


图 2 串口调试软件的设置

5.3 向 HS520A 发送命令

发送命令的格式为：起始符(STX: 0x0A) + 包序号(一般设 0x00 即可) + 命令字 + 数据长度 + 数据 + BCC 校验 + 结束符(ETX: 0x0B)。详细说明见前文。

《HS520A命令集_V1.00.txt》列出了一些常用的命令，一些可以直接拷贝到串口调试

软件的发送窗口中直接进行发送。有一些需要用户进行一定的修改，例如使用的卡片不同，发送验证密钥时应填入相应的卡号。注意如果数据有些不同，则 BCC 校验也不同。

6. Mifare 卡工作状态介绍

Mifare 卡工作状态如表 17 所列。

表17. Mifare 卡工作状态列表

状态	描述
POWER OFF (断电)	卡片不位于读卡器有效区域，由于缺少射频磁场能量而处于断电状态，卡片不工作。
IDLE (空闲)	卡片进入读卡器有效区域内，被电磁场能量激活，延迟数毫秒后将进入IDLE状态。在该状态下，卡片能够解调读卡器传来的调制信号，并能对读卡器的Reques（以IDLE或 ALL方式）命令进行应答，应答后返回卡片的类型。
READY (就绪)	卡片对读卡器的Request命令进行应答后，就进入了READY状态。在该状态中，可以采用比特帧防冲突算法。当卡片的唯一序列号被读卡器发来的Selection命令选中时，就退出本状态。
ACTIVE (激活)	当卡片的唯一序列号被读卡器选中时就进入ACTIVE状态。在该状态中，卡片完成本次应用所要求的全部操作。
HALT (停止)	卡片应用完成后，读卡器可通过发送Halt命令，使卡片进入 HALT 状态。在该状态中，卡片只对读卡器以ALL方式发送的 Request命令进行应答（或被唤醒），从而又进入READY状态。

图 3 为 Mifare 卡的状态转换图。

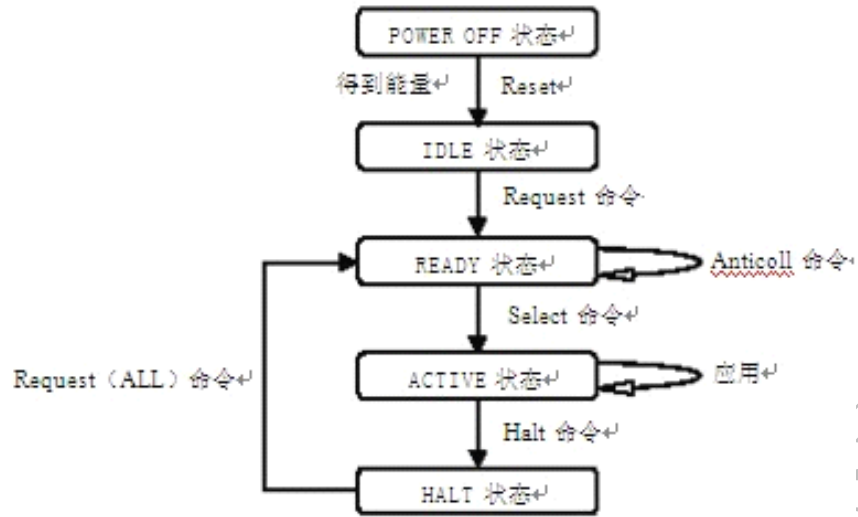


图 3 Mifare 卡状态转换示意图

深圳华视电子读写设备有限公司