目　录

第1章 Mifare522 Module 使用说明书

1.1 硬件描述

MIFARE522_MODULE 实物图如图 1 所示。

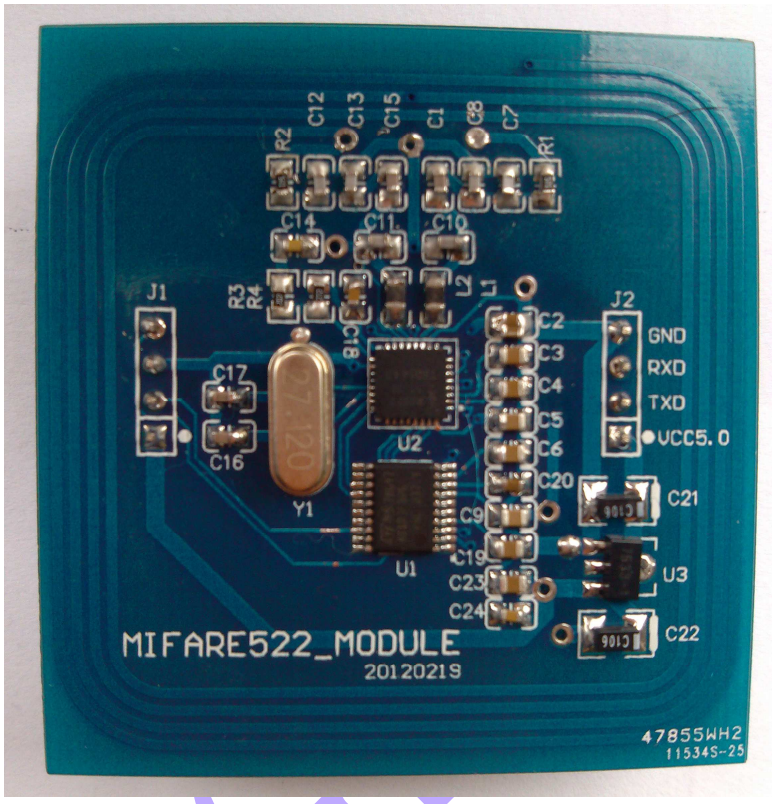

图 1 MIFARE522_MODULE 实物图

该模块的供电电压为直流 5~9V，UART TTL 电平输出。接线简单，图 1 中 J2 为接线引脚，J1 为生产编程引脚（用户不需要理会）。J2 的引脚描述如表 1 所示。

表 1 J2 的引脚描述

引脚	描述
VCC5.0	电源正极入输，5~9V
TXD	模块数据输出，接 MCU 的 RXD
RXD	模块数据输入，接 MCU 的 TXD
GND	电源地

机械结构图如图 2 所示，单位为毫米。

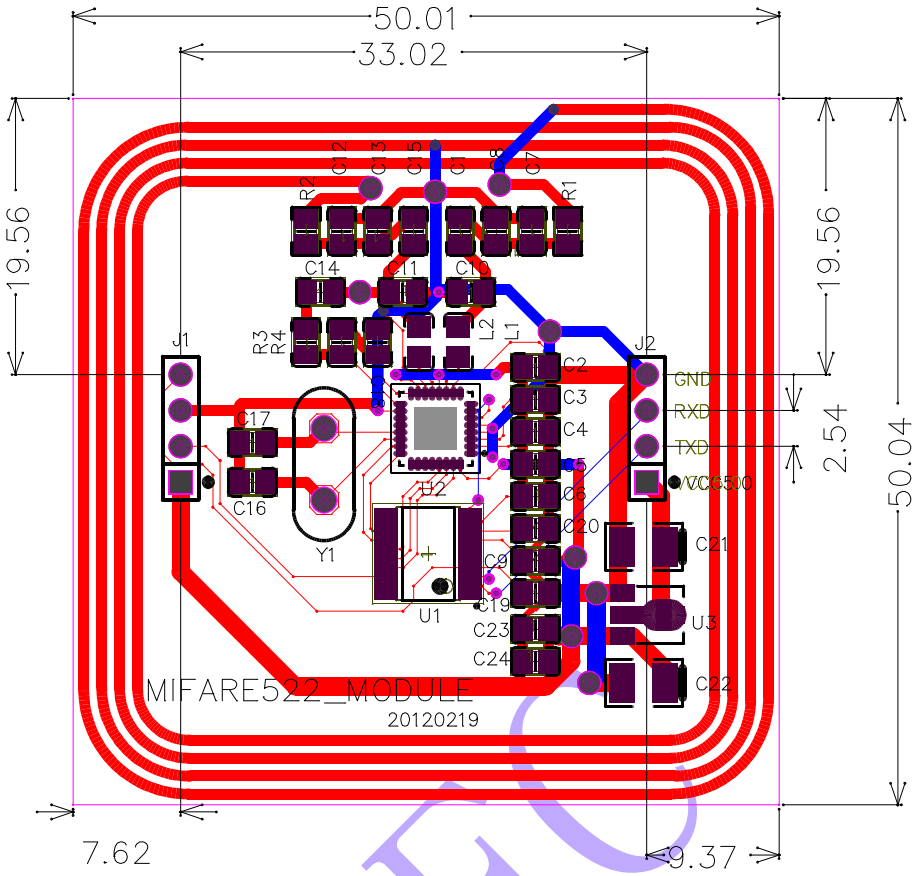

图 2 机械结构图

1.2 通信协议

本模块以命令——响应的方式工作，在系统中模块是处于从属地位，不会主动发出数据（自动检测卡片除外）。通常主机首先发出命令，然后等待模块响应。

通信控制符描述如表 2 所示。

表 2 通信控制符表

描述	定义	值
开始符	STX	0x20
终止符	ETX	0x03
应答	ACK	0x06
无应答	NAK	0x15

UART 接口一帧的数据格式为 1 个起始位，8 个数据位、无奇偶校验位、1 个停止位，波特率固定为 9600。

数据帧

数据总是以一帧为单位进行通信的，一帧的数据格式如下：

帧长 FrameLen	包号/命令类型 SEQ/CmdType	命令/状态 Cmd/Status	信息长度 Length	信息 Info	校验和 BCC	帧结束符 ETX
1byte	1byte	1byte	1byte	N bytes	1byte	1byte

网络层字段说明如表 3所示：

表 3 数据帧各字段说明表

字段	长度	说明	补充
FrameLen	1	数据帧的长度，包含它自己。	
SEQ/ CmdType	1	Bit 7-4：该包序号，从 0 到 15 循环。可以用来作为通信间的错误检查，从机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
		Bit 3-0：命令类型。 0x00：协议控制类命令，如设置地址、读产品序号等 0x01：设备控制类命令，如读写 IO、控制蜂鸣器、读写寄存器等 0x02：ISO14443A 命令 其他值保留。 从机返回相同的 CmdType	
Cmd/ Status	1	主机——从机：命令 从机——主机：状态	
Length	1	该帧所带数据信息长度 若模块返回状态不为 0，则 Length=0。	
Info	Length	数据信息	

BCC	1	校验和。从 FrameLen 开始到 Info 的最后一字节异或取反，C 语言程序描述如下：（SerBfr 为一帧数据缓冲区首址）
		BCC = 0;
		for(i=0; i<(SerBfr[0]-2); i++) {
		BCC ^= SerBfr[i];
		}
		SerBfr[SerBfr[0]-2] = ~BCC;	

ETX	1	0x03：“End of Text”标准的控制字符，是一个帧的结束标志	

数据帧接收规则：

- 一帧的结束一定是 ETX，但接收到0x03 则不一定是帧结束；
- 帧长必须不小于 6 字节，最大不能超过54 字节，且帧长必须等于信息长度加6；
- BCC 计算必须正确。

无论是主机还是从机所接收的数据必须符合以上规则，否则从机不会执行任何命令，也不会有任何错误响应，主机也必须丢弃这帧数据，以找出错误原因，从而纠正错误。

1.3 应用命令详述

1.3.1 设备控制类命令（CmdType = 1）

设备控制类命令总汇如表 4所示。

表 4 设备控制类命令一览表

命令符	意义
A	读设备信息—GetDvcInfo
B	配置读卡芯片—PCDConfig
C	关闭读卡芯片—PCDClose

1. 读设备信息（**Cmd = A**）

声明： *INT8U GetDvcInfo(INT8U *DvcInfo);*

- 主机命令：

  命令类型（*CmdType*）： 0x01

  命令 （*Command*）： ‘A’

  数据长度（*Length*）： 0

  数据信息（*Info*）： none

  例如：

  数据帧：

FrameLen	CType	Cmd	Length	Info	BCC	ETX
0x06	0x01*	0x41	0x00	NONE	0xB9	0x03

*假设所有的例子中包序号SEQ 为0。

- 从机应答

  状态 （*Status*）： 0

  数据长度（*Length*）： 14

  数据信息（*Info*）： ’ZLG522S V1.06’

  例如：

  数据帧：

FrameLen	CType	Status	Length	Info	BCC	ETX
0x12	0x01	0x00	0x0C	“RC522 V1.00”	0xCD	0x03

2. 配置读卡芯片（**Cmd = B**）

声明： *INT8U PCDConfig();*

- 主机命令：

  命令类型（*CmdType*）： 0x01

  命令 （*Command*）： ‘B’

数据长度（*Length*）： 0
数据信息（*Info*）： none
例如：
数据帧：

FrameLen	CType	Cmd	Length	Info	BCC	ETX
0x06	0x01	0x42	0x00	NONE	XX	0x03

- 从机应答
  状态 （*Status*）： 0——成功，其它——失败
  数据长度（*Length*）： 0
  数据信息（*Info*）： none
  例如：
  数据帧：

FrameLen	CType	Status	Length	Info	BCC	ETX
0x06	0x01	0x00	0x00	NONE	XX	0x03

3. 关闭读卡芯片（**Cmd = C**）

声明： *INT8U PCDClose();*

- 主机命令：
  命令类型（*CmdType*）： 0x01
  命令 （*Command*）： *‘C’*
  数据长度（*Length*）： 0
  数据信息（*Info*）： none
  例如：
  数据帧：

FrameLen	CType	Cmd	Length	Info	BCC	ETX
0x06	0x01	0x43	0x00	NONE	XX	0x03

- 从机应答
  状态 （*Status*）： 0——成功，其它——失败
  数据长度（*Length*）： 0
  数据信息（*Info*）： none
  例如：
  数据帧：

FrameLen	CType	Status	Length	Info	BCC	ETX
0x06	0x01	0x00	0x00	NONE	XX	0x03

1.3.2 ISO14443A 类命令（CmdType = 2）

ISO14443A类命令总汇如表 5所示。

表 5 ISO14443A 类命令一览表

命令符	意义
A	请求—Request
B	防碰撞—CascAnticoll
C	选择—CascSelect
D	卡挂起—Halt
E	证实 E2—Authentication
F	证实—AuthKey
G	读—Read
H	写—Write

前4 条命令（命令A—D）是ISO14443A 标准定义的命令，只要符合该标准的卡都应能发出响应；中间4条命令（命令E—H）为Mifare1 卡的专用命令，只有先进行验证（命令E、F）成功之后才能进行。

1. 请求（Cmd = A）

声明： *INT8U PiccRequest(INT8U Req_Code,INT8U *TagType);*

- 主机命令：

  命令类型（*CmdType*）： 0x02

  命令 （*Command*）： ‘A’

  数据长度（*Length*）： 1

  数据信息（*Info*）： 请求模式（1 字节）： 0x26——IDLE

  0x52——ALL

  例如：请求天线范围内所有的卡

  数据帧：

FrameLen	CType	Cmd	Length	Info	BCC	ETX
0x07	0x02	0x41	0x01	52	XX	0x03

- 从机应答

  状态 （*Status*）： 0——成功，其它——失败

  数据长度（*Length*）： 2

  数据信息（*Info*）： 请求应答ATQ（2 字节，低字节在前）

b15	b14	b13	b12	b11	b10	b9	b8	b7	b6	b5	b4	b3	b2	b1	b0
RFU								UID 大小 00:4bytes 01:7bytes 10:10bytes		RFU	如果有任何位为 1，则为比特帧防冲突方式				

表 6例举了各种类型的卡返回的ATQ。

表 6 返回 ATQ 一览表

卡类型	ATQ	卡类型	ATQ
Mifare1 S50	0x0004	SHC1101	0x0004
Mifare1 S70	0x0002	SHC1102	0x3300
Mifare1 Light	0x0010	11RF32	0x0004
Mifare0 UltraLight	0x0044	Mifare3 DESFire	0x0344

例如：S50 卡返回的ATQ

数据帧：

FrameLen	CType	Status	Length	Info	BCC	ETX
0x08	0x02	0x00	0x02	0x04 0x00	XX	0x03

- 说明

卡进入天线后，从射频场中获取能量，从而得电复位，复位后卡处于IDLE 模式，用两种请求模式的任一种请求时，此时的卡均能响应；若对某一张卡成功进行了挂起操作（Halt命令或DeSelect*命令），则进入了Halt 模式，此时的卡只响应ALL（0x52）模式的请求，除非将卡离开天线感应区后再进入。*注：DeSelect 为ISO14443-4 命令。

另外，对Mifare1 卡连续进行请求操作，总是一次成功，一次失败，循环往复。

2. 防碰撞（Cmd = B）

声明： *INT8U PiccAnticoll(INT8U Sel_Code,INT8U Bcnt,INT8U *PiccSnr);*

- 主机命令：

命令类型（*CmdType*）： 0x02

命令 （*Command*）： ‘B’

数据长度（*Length*）： 若位计数=0，则长度=2

若位计数≠0，则长度=6

数据信息（*Info*）： 选择代码（1 字节）： 0x93——第一级防碰撞

0x95——第二级防碰撞

0x97——第三级防碰撞

位计数（1 字节）： 已知的序列号的长度

序列号（4 字节）（若位计数≠0）

例如：第一级防碰撞

数据帧：

FrameLen	CType	Cmd	Length	Info	BCC	ETX
0x08	0x02	0x42	0x02	0x93 0x00	XX	0x03

- 从机应答

状态 （*Status*）： 0——成功，其它——失败

数据长度（*Length*）： 4

数据信息（*Info*）： UID（4 字节，低字节在先），若UID 不完整，则最低字节为级联标志0x88，需要进行更高一级的防碰撞。

例如：返回序列号0x8e6e8610

FrameLen	CType	Status	Length	Info	BCC	ETX
0x0A	0x02	0x00	0x04	0x10 0x86 0x6e 0x8e	XX	0x03

- 说明

符合ISO14443A 标准卡的序列号都是全球唯一的，正是这种唯一性，才能实现防碰撞的算法逻辑，若有若干张卡同时在天线感应区内则这个函数能够找到一张序列号较大的卡来操作。实际上由于天线辐射的磁场能量有限，同时在天线感应区内的所有卡都要从辐射场中吸收，因此同时在天线感应区内的卡不能太多，否则辐射场能量被平分，没有一张卡能获得足够的能量来正常工作。

位计数为已知的序列号的位数，若位计数=0，则序列号的所有位都要从本函数获得；若位计数≠0，则序列号中有已知的序列号的值，表示要获得序列号的前位计数位为序列号中所示的卡的其余位的值。位计数必须小于32，若位计数等于32，则可直接用选择命令，选择一张已知序列号的卡。

3. 选择（Cmd = C）

声明： *INT8U PiccSelect(INT8U Sel_Code,INT8U *PiccSnr,INT8U *Sak);*

- 主机命令：

命令类型（*CmdType*）： 0x02
命令 （*Command*）： ‘C’
数据长度（*Length*）： 5
数据信息（*Info*）： 选择代码（1 字节）： 0x93——第一级防碰撞
0x95——第二级防碰撞
0x97——第三级防碰撞
UID（4 字节）：前一个防碰撞命令返回的UID（包含级联志）

例如：第一级选择，UID 为0x8e6e8610

数据帧：

FrameLen	CType	Cmd	Length	Info	BCC	ETX
0x0B	0x02	0x43	0x05	0x10 0x86 0x6e 0x8e	XX	0x03

- 从机应答

状态 （*Status*）： 0——成功，其它——失败
数据长度（*Length*）： 1
数据信息（*Info*）： 选择应答 SAK

b7	b6	b5	b4	b3	b2	b1	b0
RFU			RFU			RFU	

b2：Cascade 位，表示UID 是否完整，
若b2=0，表示UID 完整；
若b2=1，表示UID 不完整，还有部分UID 未读出。

表 7例举了各种类型的卡第一级选择返回的SAK

表 7 返回 SAK 一览表

卡类型	ATQ	卡类型	ATQ
Mifare1 S50	0x08	SHC1101	0x22
Mifare1 S70	0x18	SHC1102	
Mifare1 Light	0x01	11RF32	0x08
Mifare0 UltraLight	0x04		
Mifare3 DESFire	0x24		

例如：选择 S50 卡应答

FrameLen	CType	Status	Length	Info	BCC	ETX
0x07	0x02	0x00	0x01	0x08	XX	0x03

- 说明

卡的序列号长度有三种：4 字节、7 字节和10 字节。4 字节的只要用一级选择即可得到完整的序列号，如Mifare1 S50 S70 等；7 字节的要用二级选择才能得到完整的序列号，前一级所得到的序列号的最低字节为级联标志0x88，在序列号内只后3 字节可用，后一级选择能得到4 字节序列号，两者按顺序连接即为7 字节序列号，如UltraLight 和DesFire 等；10 字节的以此类推，但至今还未发现此类卡。

在程序中可用 SAK.2 位来判断是还有序列号未读出，如 if(SAK & 0x04){…}。

4. 暂停（Cmd = D）

声明： *INT8U PiccHalt();*

- 主机命令：

命令类型（*CmdType*）： 0x02
命令 （*Command*）： ‘D’
数据长度（*Length*）： 0
数据信息（*Info*）： none
例如：
数据帧：

FrameLen	CType	Cmd	Length	Info	BCC	ETX
0x06	0x02	0x44	0x00	NONE	XX	0x03

- 从机应答

状态 （*Status*）： 0——成功，其它——失败

数据长度（*Length*）： 0

数据信息（*Info*）： none

例如：

数据帧：

FrameLen	CType	Status	Length	Info	BCC	ETX
0x06	0x02	0x00	0x00	NONE	XX	0x03

- 说明

此命令将使所选择的卡进入Halt 状态，在Halt 状态下，卡将不响应读卡器发出的IDLE模式的请求，除非将卡复位或离开天线感应区后再进入。但它会响应读卡器发出的ALL 请求。

5. 直接密码证实（Cmd = F）

声明： *INT8U PiccAuthKey(INT8U KeyAB,INT8U *PiccSnr,INT8U *Key,INT8U Block);*

- 主机命令：

命令类型（*CmdType*）： 0x02

命令 （*Command*）： ‘F’

数据长度（*Length*）： 12

数据信息（*Info*）： 密钥AB（1 字节）： 0x60——密钥A

0x61——密钥B

卡序列号（4 字节）

密钥（6 字节）

卡块号（1 字节）： S50：0——63

S70：0——255

例如：用密钥“0xFF 0xFF 0xFF 0xFF 0xFF 0xFF”证实序列号为0x8e6e8610的卡的块4的密钥A

数据帧：

FrameLen	CType	Cmd	Length	Info	BCC	ETX
0x12	0x02	0x46	0x0C	0x10 0x86 0x6e 0x8e 0xFF 0xFF 0xFF 0xFF 0xFF 0xFF 0x04	XX	0x03

- 从机应答

状态 （*Status*）： 0——成功，其它——失败

数据长度（*Length*）： 0

数据信息（*Info*）： none

例如：

数据帧：

FrameLen	CType	Status	Length	Info	BCC	ETX
0x06	0x02	0x00	0x00	NONE	XX	0x03

6. 读（Cmd = G）

声明： *INT8U PiccRead(INT8U Block,INT8U *Bfr);*

- 主机命令：

  命令类型（*CmdType*）： 0x02

  命令 （*Command*）： ‘G’

  数据长度（*Length*）： 1

  数据信息（*Info*）： 卡块号（1 字节）： S50：0——63

  S70：0——255

  例如：读块4 数据

  数据帧：

FrameLen	CType	Cmd	Length	Info	BCC	ETX
0x07	0x02	0x47	0x01	0x04	XX	0x03

- 从机应答

  状态 （*Status*）： 0——成功，其它——失败

  数据长度（*Length*）： 16

  数据信息（*Info*）： 块数据（16 字节）

  例如：

  数据帧：

FrameLen	CType	Status	Length	Info	BCC	ETX
0x16	0x02	0x00	0x10	0x05 0x05 0x05 0x05 0x05 0x05 0x05 0x05 0x05 0x05 0x05 0x05 0x05 0x05 0x05 0x050x05 0x05	XX	0x03

- 说明

在验证成功之后，才能读相应的块数据，所验证的块号与读块号必须在同一个扇区内，Mifare1 卡从块号0 开始按顺序每4 个块1 个扇区。

若要对一张卡中的多个扇区进行操作，在对某一扇区操作完毕后，必须进行一条读命令才能对另一个扇区直接进行验证命令，否则必须从请求开始操作。

7. 写（Cmd = H）

声明： *INT8U PiccWrite(INT8U Block,INT8U *Bfr);*

- 主机命令：

  命令类型（*CmdType*）： 0x02

  命令 （*Command*）： ‘H’

  数据长度（*Length*）： 17

  数据信息（*Info*）： 卡块号（1 字节）： S50：0～63

  S70：0～255

  数据（16 字节）

  例如：写块4 数据

  数据帧：

FrameLen	CType	Cmd	Length	Info	BCC	ETX
0x17	0x02	0x48	0x11	0x04 0x05 0x05 0x05 0x05 0x05 0x05 0x05 0x05 0x05 0x05 0x05 0x05 0x05 0x05 0x05 0x05	XX	0x03

- 从机应答

  状态 （*Status*）： 0——成功，其它——失败

  数据长度（*Length*）： 0

  数据信息（*Info*）： none

  例如：

  数据帧：

FrameLen	CType	Status	Length	Info	BCC	ETX
0x06	0x02	0x00	0x00	NONE	XX	0x03

- 说明

对卡内某一块进行验证成功后，即可对同一扇区的各个进行写操作（只要访问条件允许），其中包括位于扇区尾的密码块，这是更改密码的唯一方法。

附录A S50 卡读数据流程

S50 卡读数据流程如图 3 所示。

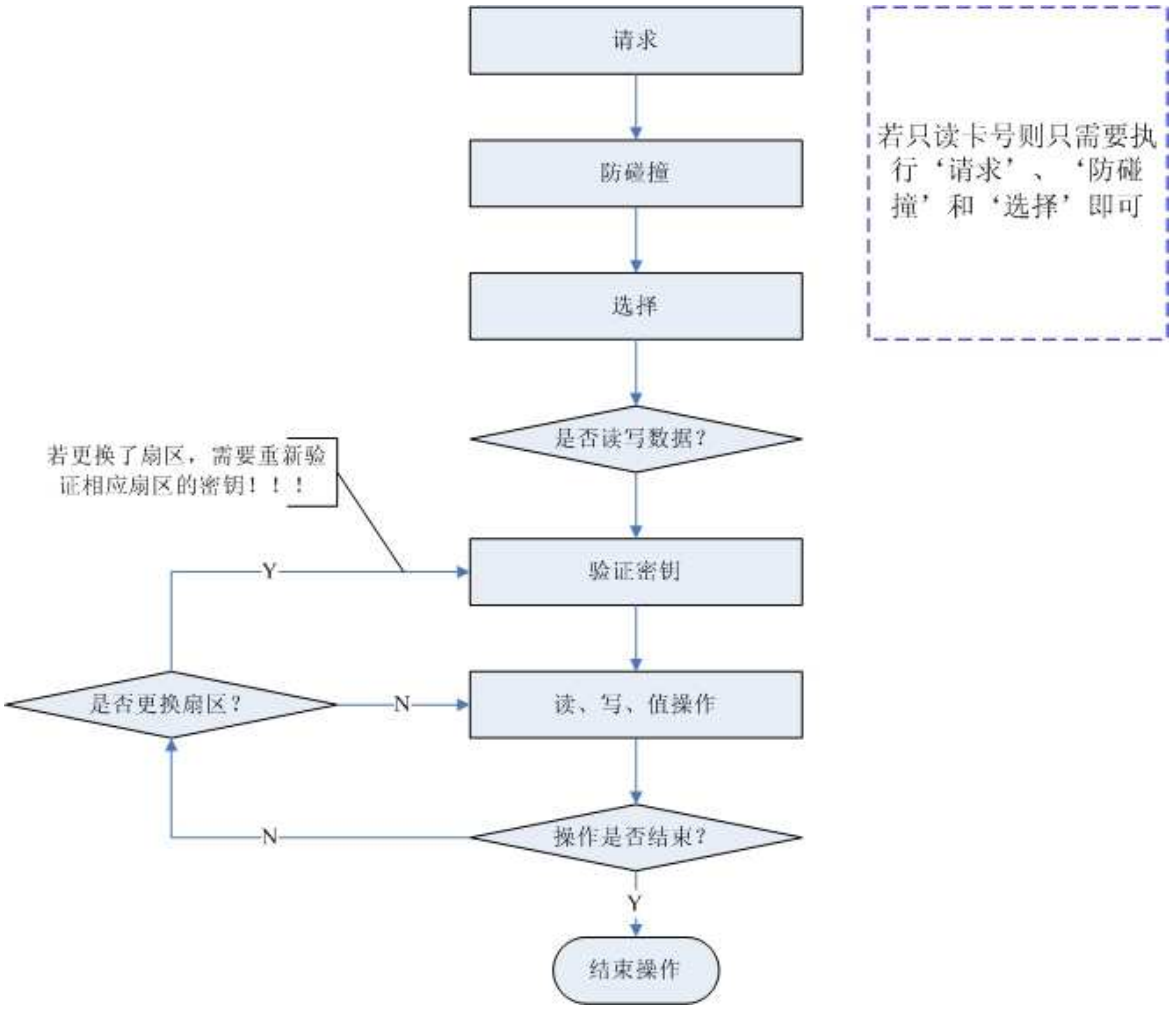

图 3 S50 卡读数据流程