上海复旦微电子股份有限公司
SHANGHAI FUDAN MICROELECTRONICS CO., LTD.

8K 位 EEPROM 非接触式射频卡芯片 FM11RF08

8kBits Contactless IC Card Chip FM11RF08

FM11RF08 是复旦微电子股份有限公司设计的非接触式射频卡芯片，采用 0.6 微米 CMOS EEPROM 工艺，容量为 1K × 8bit EEPROM，是具有逻辑处理功能的多用途非接触射频卡芯片，内含加密控制和通讯逻辑电路，具有极高的保密性能。适用于各类计费系统的支付卡的应用。

FM11RF08 is the contactless IC card chip developed by shanghai FM Co.,Ltd..It takes 0.6μm CMOS EEPROM processing technology. The chip has 1Kx8bit EEPROM organization,and is a true multi-application smart card with the functionality of a processor card realized with hardware logic,and also has a very high security performance with the encryption and communication circuit ,so FM11RF08 can be especially tailored to meet the requirements of a payment card which can be used for ticketing systems in public transport and comparable applications.

产品特点

- 1024 × 8bit EEPROM 存储单元
- 工作频率为 13.56MHz
- 通讯波特率为 106K
- 操作距离不小于 10cm
- 半双工通讯方式
- 高度安全的数据通信
- 具有安全保护结构的 16 个独立的扇区，支持多种应用
- 对于使用分级密钥的系统，每个扇区都可拥有两套独立的密钥
- 对存储单元的访问权限可由用户根据自身的要求灵活定义
- 算术功能：进行加减法运算
- 高可靠的 EEPROM 读写控制电路，大于 10 万次的擦写测试，10 年数据保存期
- 符合 ISO/IEC 14443

FEATURES

- 1024x 8bit EEPROM memory, no battery.
- 13.56MHz operating frequency
- 106K communication baudrate
- The permissible distance between antenna and card is up to 100mm free air.
- Half duplex communication protocol using handshake
- High security level data communication
- Organized in security separated 16 sectors supporting multiapplication use.
- Each sector has its own two secret files for systems using key hierarchies.
- User flexible defines assess conditions for each memory block.
- Arithmetic capability: increase and decrease.
- More than one hundred thousand write test,data retention of 10 years
- Compatible with ISO/IEC 14443

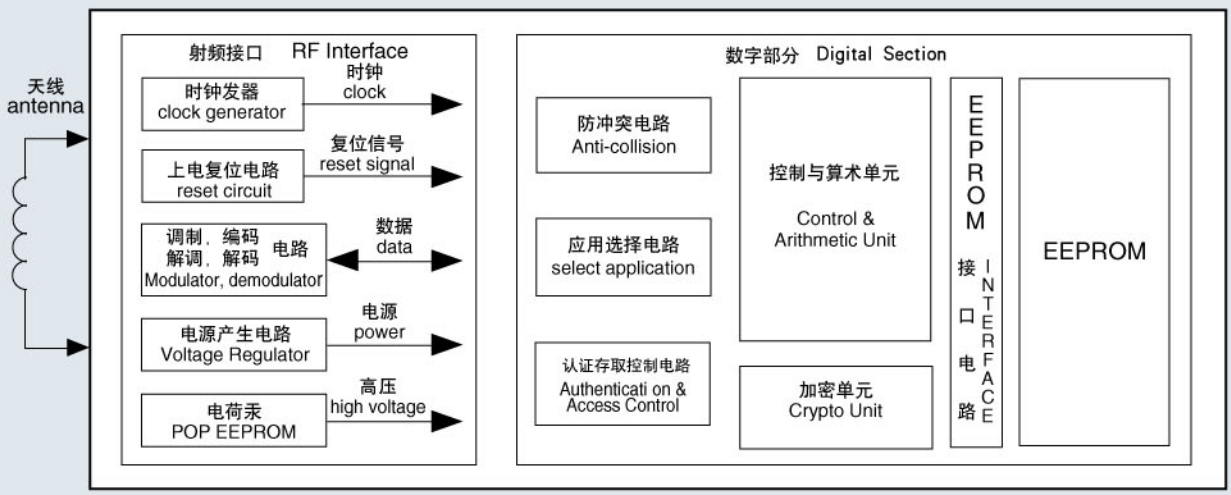
典型处理时间:

- 识别一张卡 3ms （包括复位应答和防冲突）
- 读一个块 2.5ms （不包括认证过程）
- 写一个块＋读操作 12ms （不包括认证过程）
  14ms （包括认证过程）
- 典型交易过程 <100ms

Typical Transaction Time

- Identification of a card 3ms (incl.Answer to request and Anti-collision)
- Read Block (16bytes) 2.5ms(excl. Authentication)
- Write Block +Control Read 12ms(excl.Authentication)
  14ms(incl.Authentication)
- Typical Ticketing Transaction <100ms

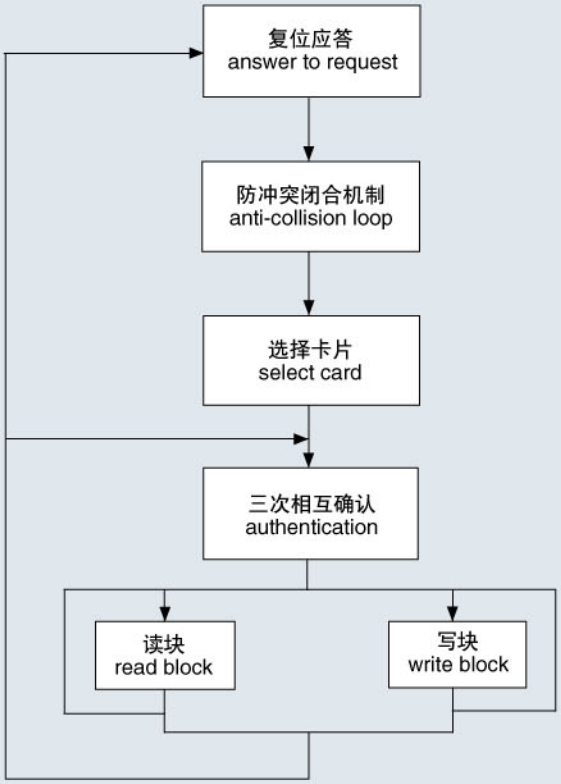
结构框图 BLOCK DIAGRAM :



产品功能：FUNCTION DESCRIPTION

一．FM11RF08射频卡与读写器之间的操作流程

Transaction sequenece:



复位应答

FM11RF08 射频卡的通讯协议和通讯波特率是定义好的，通过这两项内容，读写器和FM11RF08卡相互验证。当某张卡片进入读写器的操作范围时，读写器以特定的协议与它通讯，从而确定该卡是否为FM11RF08射频卡，即验证卡片的卡型。

Answer to Request

The type of a card defines the communication protocol and the communication baudrate between RWD and card. When a card is in the operating range of a RWD, the RWD continues communication with the appropriate protocol, specified by the type of a card.

防冲突闭合机制

当有多张 FM11RF08 卡在读写器的操作范围内时，防冲突闭合电路首先从众多卡片中选择其中的一张作为下一步处理的对象，而未选中的卡片则处于空闲模式以等待下一步被选择，该过程返回一个被选中的卡的序列号。

Anti-collision Loop

If there are several cards in the operating range of RWD they can be distinguished by their different serial numbers and one can be selected for further transactions. The unselected cards return to the standby mode and wait for a new Answer to Request and Anti-collision loop.

选择卡片

选择被选中的卡的序列号，卡片返回选择确认编码（SAK）。

Select Card

After selection of a card, the card returns the Answer To Select code (SAK).

三次互相确认

选定要处理的卡片之后，读写器就确定要访问的扇区号，并对该扇区密码进行密码校验，在三次互相认证之后就可以通过加密流进行任何通讯。（在选择下一个扇区时，则必须进行新扇区的密码校验。）

3 Pass Authentication

After Selection of a card, RWD specifies the memory location of the following memory access and use the corresponding key for the 3 Pass Authentication procedure. Any communication after authentication is performed via stream cipher encryption.

读／写

确认之后就可以执行下列操作:

读：读一个块

写：写一个块

减：块中的内容作减法之后，结果存在数据寄存器中

加：块中的内容作加法之后，结果存在数据寄存器中

传输：将数据寄存器中的内容写入块中

存储：将块中的内容读到数据寄存器中

暂停：将卡置于暂停工作状态

Read/Write

After authentication of the following operations may be performed:

READ:	read one block
WRITE:	write one block
DECREMENT:	decrements the contents of one block and stores the result in the data-register
INCREMENT:	increments the contents of one block and stores the result in the data-register
TRANSFER:	writes the contents of the data-register to one block
RESTORE:	stores the contents of one block in the data-register
Halt:	pause operation

二．指令集 Commands aggregation:

指令名称 Commands	指令代码 Code(16 进制)
寻找未被置成暂停状态的卡 request std	26
寻找所有在操作区域内的卡 request all	52
防冲突指令 Anti-collision	93
选择卡片指令 Select Card	93
验证密码 A Authentication.1a	60
验证密码 B Authentication.1b	61
读块指令 Read	30
写块指令 Write	A0
加法指令 Increment	C1
减法指令 Decrement	C0
存储指令 Restore	C2
传输指令 Transfer	B0
暂停指令 Halt	50

三．数据的完整性

在非接触通讯中，以下措施保证了读写器和卡片之间数据传递的完整、可靠;

- 防冲突
- 每块有 16 位 CRC 纠错
- 每个字节有奇偶校验位
- 检查位数
- 用编码方式来区分“1”，“0”或无信息
- 信道监测（通过协议顺序和位流分析）

Data Integrity

Following mechanisms are implemented in the contactless communicaton link between RWD and card to ensure very reliable data transmission:

- Anti-collision
- 16 bit CRC per block
- Parity bits for each byte
- Bit count checking
- Bit coding to distinguish between "1", "0", and no information
- Channel monitoring (Protocol sequence and bit stream analysis)

四．保密性

FM11RF08射频卡的良好保密性能是在于: 读写前的三次相互认证过程、每张卡不同的卡片序列号、传递数据加密、传递密码和访问密码保护。

卡片中的密码是受保护的、不可读的、只有知道密码的用户才能修改它。卡中的 EEPROM 存储区分为 16 个扇区，每个扇区都有自己的密码，用户可根据扇区的不同应用设定不同的密码（一卡多用）。扇区的访问密码分为 KEYA 和 KEYB 两组不同密码，根据访问条件，在校验 KEYA 或 KEYB 之后才可以对存储器进行访问。

Security:

The FM11RF08 Card has high security: 3 PASS Authentication must be through before read/write operation. Serial Numbers, which can not be altered, guarantee the uniqueness of each card. Crypto-Data transfer, Key Transfer and Access Key Protection.

Keys in the cards are read protected but can be altered by who knows the actual key. There are 16 sectors in the card, each sector has own keys(Key A ,Key B). Two different keys for each sector support systems using key hierarchies , so FM11RF08 offers real multi-application functionality.

五．存储区的结构和访问条件

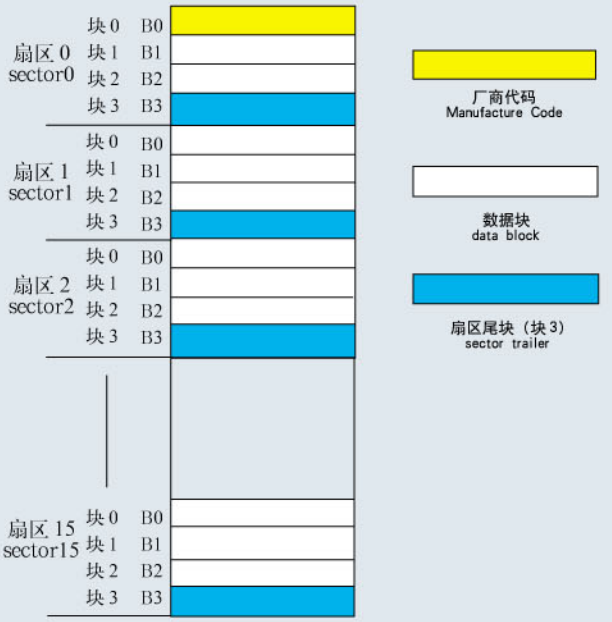
FM11RF08射频卡的8Kbits EEPROM分为16个扇区，每个扇区由 4 个数据块组成，每块有 16 个字节。

Memory Organization and Access Conditions

The 1024 × 8bit EEPROM memory is organized in 16 sectors with 4 block of 16 bytes each.

存储区的分区如下图所示:

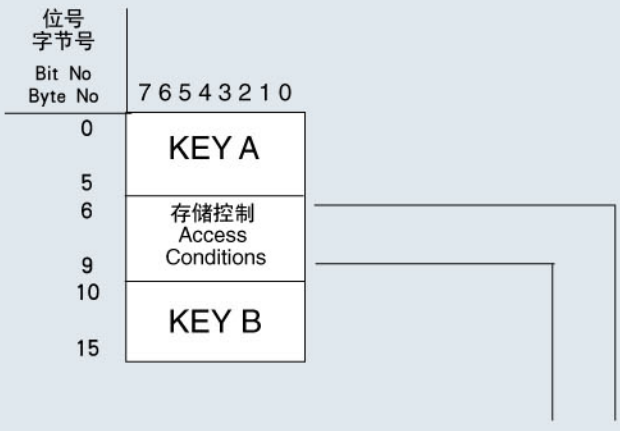
the structure of memory is shown below:



每个扇区的块 3 包含了该扇区的密码 A（6 个字节）、存取控制（4 个字节）和密码 B（六个字节），是一个特殊的块，其余三块是一般的数据块。但是，扇区 0 的块 0 是特殊的，它用于存放厂商的代码比如 32 位的序列号，已经固化，只可读不可更改。 数据块有两种应用：用作一般的数据保存使用，直接读写；以特殊数据格式表示时，可以进行初始化赋值、加值、减值和读值。块 3 的结构如下图所示:

The fourth block of any sector contains access KEYA (6 bytes)、an optional KEYB(6 bytes) and the access conditions for the four blocks of that sector(4 bytes). The other blocks of the sector serve as common data blocks. The first block of the memory is reserved for manufacturer data like 32 bit serial number. This is a read only block. In many documents it is named "block0"

The structure of block3 is shown below:



Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
C2X3_b	C2X2_b	C2X1_b	C2X0_b	C1X3_b	C1X2_b	C1X1_b	C1X0_b
C1X3	C1X2	C1X1	C1X0	C3X3_b	C3X2_b	C3X1_b	C3X0_b
C3X3	C3X2	C3X1	C3X0	C2X3	C2X2	C2X1	C2X0
BX7	BX6	BX5	BX4	BX3	BX2	BX1	BX0

_b 表示取反，如 C2X3_b 即 C2X3 取反;

X 表示扇区号；Y 表示第几块；C 表示控制位；B 表示备用位;

_b stands for inversion e.g.:C2X3_b=INV(C2X3)

X stands for sector No.(0 ~ 15)

Y stands for block No.(0 ~ 3)

表 2 存取控制对块 3 的控制如下:

(X=0 ~ 15) Access condition for the Sector Trailer(Y=3)

			密码 A Key A	密码 A Key A	存取控制 Access Con	存取控制 Access Con	密码 B Key B	密码 B Key B
C1X3	C2X3	C3X3	Read	Write	Read	Write	Read	Write
0	0	0	Never	KEYA|B	KEYA|B	Never	KEYA|B	KEYA|B
0	1	0	Never	Never	KEYA|B	Never	KEYA|B	Never
1	0	0	Never	KEYB	KEYA|B	Never	Never	KEYB
1	1	0	Never	Nerer	KEYA|B	Never	Never	Never
0	0	1	Never	KEYA|B	KEYA|B	KEYA|B	KEYA|B	KEYA|B
0	1	1	Never	KEYB	KEYA|B	KEYB	Never	KEYB
1	0	1	Never	Never	KEYA|B	KEYB	Never	Never
1	1	1	Never	Never	KEYA|B	Never	Never	Never

注: KEYA|B 表示密码 A 或密码 B;

Never 表示没有条件实现;

Note: KEY A|B means KEY A or KEY B,

Never means can't perform the function.

表 3 数据块的存储控制

Access condition for Data Blocks (X=0 ~ 15 Y=0 ~ 2)

C1XY	C2XY	C3XY	Read	Write	Increment	decr.transfer.restore
0	0	0	KEYA|B	KEYA|B	KEYA|B	KEYA|B
0	1	0	KEYA|B	Never	Never	Never
1	0	0	KEYA|B	KEYB	Never	Never
1	1	0	KEYA|B	KEYB	KEYB	KEYA|B
0	0	1	KEYA|B	Never	Never	KEYA|B
0	1	1	KEYB	KEYB	Never	Never
1	0	1	KEYB	Never	Never	Never
1	1	1	Never	Never	Never	Never

地址: 上海市北京东路 668 号 C 区 7 楼
Addr: Floor 7th, Building C, 668 Eastern Beijing Road, Shanghai, China
深圳办事处 (Shenzhen Office)
Tel: +86-21-5308 5050
http:// www.fmsh.com
Tel: +86-755-328 3359
Fax: +86-21-5308 6456
Post: 200001
Fax:+86-755-369 1985