



复旦微电子

FM11RF32M ***32K 位 EEPROM 非接触式射频卡芯片***

技术手册

2013. 09

本资料是为了让用户根据用途选择合适的上海复旦微电子集团股份有限公司（以下简称复旦微电子）的产品而提供的参考资料，不转让属于复旦微电子或者第三者所有的知识产权以及其他权利的许可。

在使用本资料所记载的信息最终做出有关信息和产品是否适用的判断前，请您务必将所有信息作为一个整体系统来进行评价。采购方对于选择与使用本文描述的复旦微电子的产品和服务全权负责，复旦微电子不承担采购方选择与使用本文描述的产品和服务的责任。除非以书面形式明确地认可，复旦微电子的产品不推荐、不授权、不担保用于包括军事、航空、航天、救生及生命维持系统在内的，由于失效或故障可能导致人身伤亡、严重的财产或环境损失的产品或系统中。

未经复旦微电子的许可，不得翻印或者复制全部或部分本资料的内容。

今后日常的产品更新会在适当的时候发布，恕不另行通知。在购买本资料所记载的产品时，请预先向复旦微电子在当地的销售办事处确认最新信息，并请您通过各种方式关注复旦微电子公布的信息，包括复旦微电子的网站(<http://www.fmsh.com/>)。

如果您需要了解有关本资料所记载的信息或产品的详情，请与上海复旦微电子集团股份有限公司在当地的销售办事处联系。

商 标

上海复旦微电子集团股份有限公司的公司名称、徽标以及“复旦”徽标均为上海复旦微电子集团股份有限公司及其分公司在中国的商标或注册商标。

上海复旦微电子集团股份有限公司在中国发布，版权所有。

1 产品综述

FM11RF32M 是复旦微电子集团股份有限公司设计的非接触卡式射频卡芯片，容量为 4Kx8Bits 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，具有较高的保密性能。适用于各类计费系统的支付卡的应用。

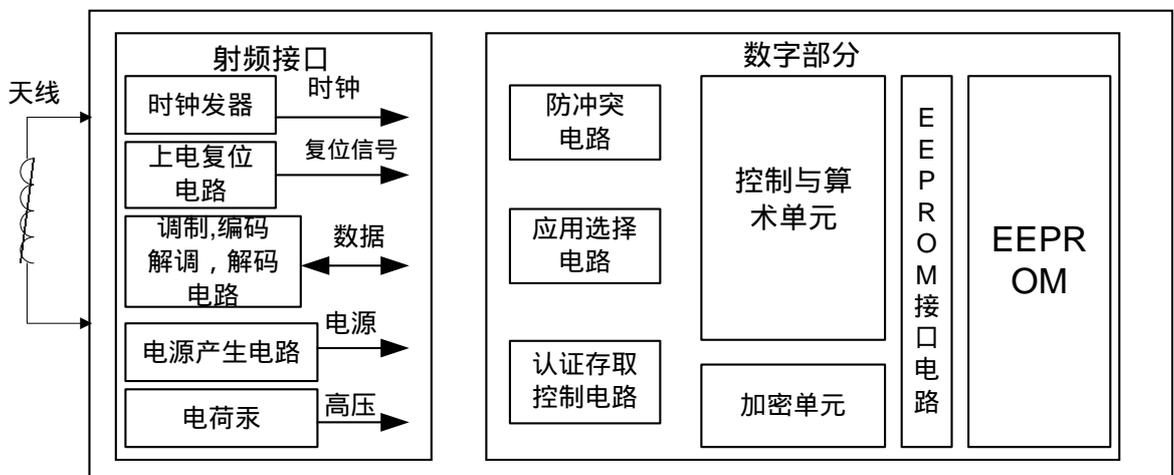
2 产品特点

4096x8bit 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（需读卡器配合）
 半双工通讯方式
 加密算法采用 M1 算法
 可靠的数据通信的安全保障技术
 具有安全保护结构的 64 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

典型处理时间：

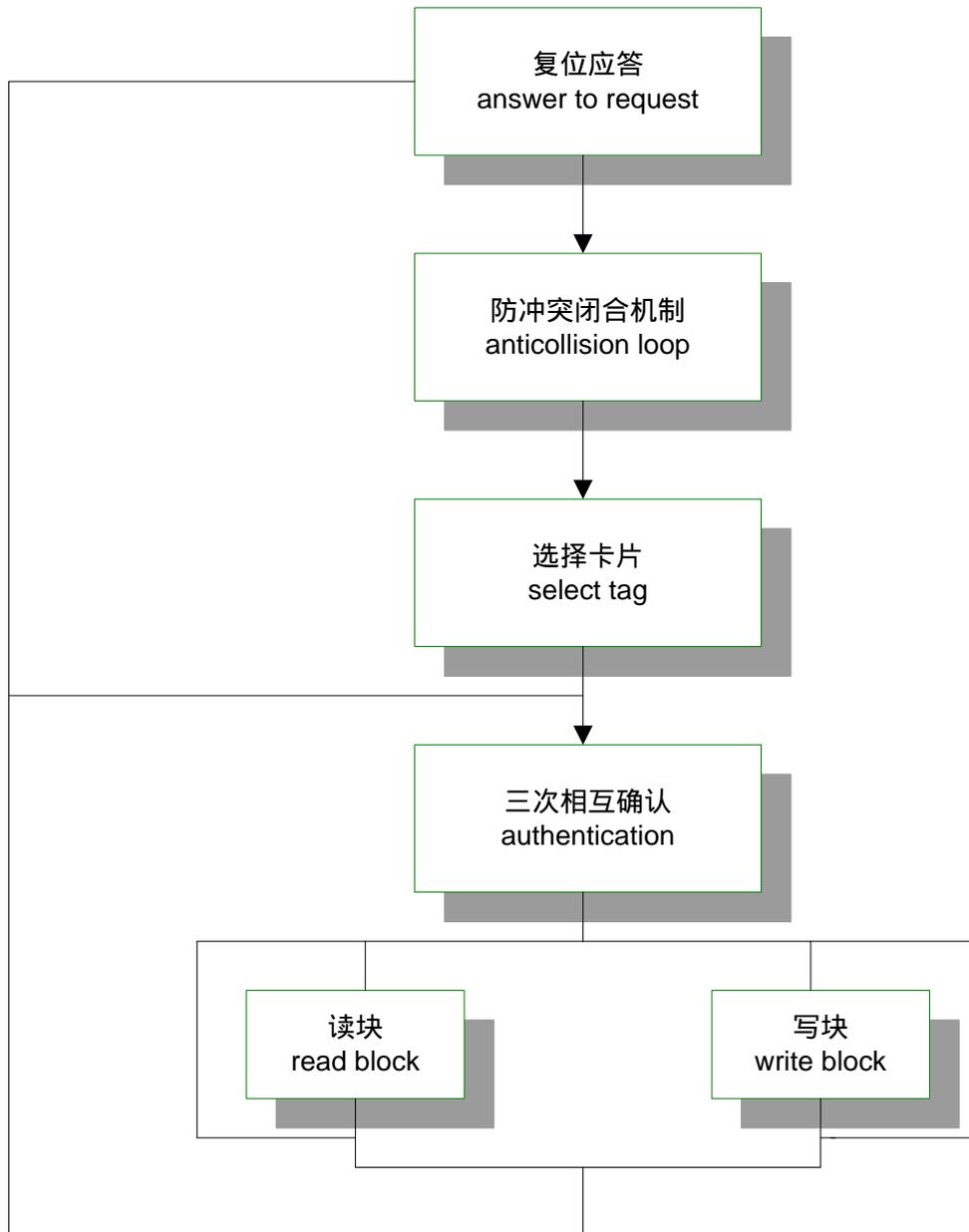
识别一张卡 3ms（包括复位应答和防冲突）
 读一个块 2.5ms（不包括认证过程）
 写一个块 + 读操作
 12ms（不包括认证过程）
 14ms（包括认证过程）
 典型交易过程 <100ms

2.1 结构框图



3 产品功能

3.1 射频卡与读写器之间的操作流程



复位应答

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，读写器和射频卡相互验证。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 FM11RF32M 射频卡，即验证卡片的卡型。

防冲突闭合机制

当有多张射频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

的卡的型号。

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。

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。）

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



4 指令集

指令名称	指令代码 (16 进制)
request std	26
request all	52
Anti-collision	93
Select Card	93
Authentication.1a	60
Authentication.1b	61
Read	30
Write	A0
Increment	C1
Decrement	C0
Restore	C2
Transfer	B0
Halt	50

5 指令说明

Answer to Request 复位应答指令

在操作区域内寻找卡片。request std 是寻找未被置成暂停状态的卡，request all 是寻找所有在操作区域内的卡。

Anti-collision 防冲突指令

如果操作区域内有一张或多张卡片，本指令将用来从这些卡片中选出一张卡。

Select card 选择卡片指令

本指令用来在防冲突指令后建立起与选中卡的通讯。

Authentication 验证指令

在访问卡片存储区之前，用户必须证明他们操作的合法性。可以通过验证读写器内的密码与卡内的密码是否一致来获得。

Read 读块指令

读出卡中某一块的 16 个字节

write 写块指令

将数据写入卡中的某一块

Increment 加法指令

将卡中的数值块加上某一数值，并把结果存于卡内的寄存器

decrement 减法指令

将卡中的数值块减去某一数值并把结果存于卡内的寄存器

restore 存储指令

将卡内数值块的内容读到卡内的寄存器

transfer 传输指令

将卡内寄存器中的内容写入块中

halt 暂停指令

将卡片置于暂停状态

6 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）

7 保密性

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 64 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。

8 存储区的结构和访问条件

射频卡的 32Kbits EEPROM 分为 64 个扇区，每个扇区由 4 个数据块组成，每块有 16 个字节。

存储区的分区如下表所示：

扇区 Sector	块 Block	每块的 byte 号														定义	
		0	1	2	3	4	5	6	7	8	9	10	11	12	13		14
63	3	Key A						Access bits				Key B				控制块	
	2																数据块
	1																数据块
	0																数据块
...
0	3	Key A						Access bits				Key B				控制块	
	2																数据块
	1																数据块
	0																制造商 数据块 (R)

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（6 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。

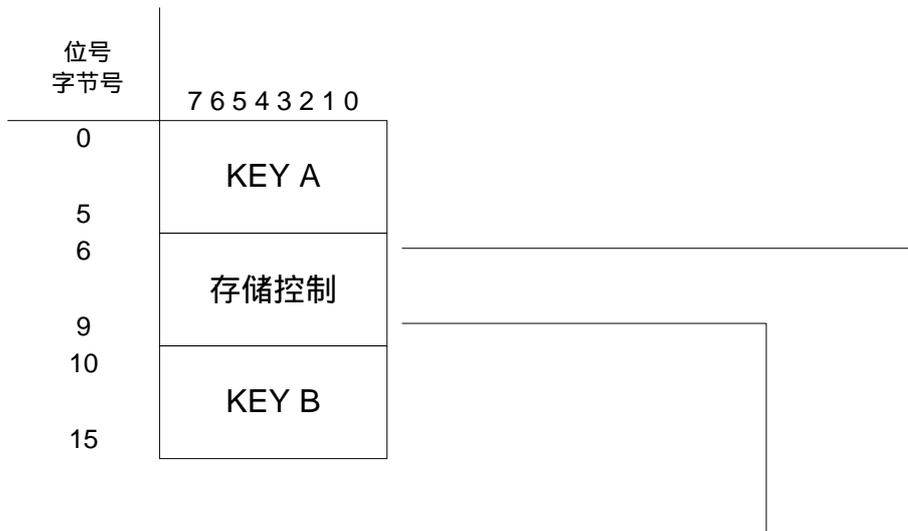
数据块有两种应用：

- 一. 用作一般的数据保存使用，直接读写；
- 二. 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。

存取控制的条件如下表所示：

控制位			有效指令	块 (扇区 0~63)	说明
C1 ₃	C2 ₃	C3 ₃	read, write	3	控制块
C1 ₂	C2 ₂	C3 ₂	read, write, increment, decrement, transfer, restore	2	数据块
C1 ₁	C2 ₁	C3 ₁	read, write, increment, decrement, transfer, restore	1	数据块
C1 ₀	C2 ₀	C3 ₀	read, write, increment, decrement, transfer, restore	0	数据块

控制块的结构如下图所示：



bit#7	bit#6	bit#5	bit#4	bit#3	bit#2	bit#1	bit#0
C2 _{3_b}	C2 _{2_b}	C2 _{1_b}	C2 _{0_b}	C1 _{3_b}	C1 _{2_b}	C1 _{1_b}	C1 _{0_b}
C1 ₃	C1 ₂	C1 ₁	C1 ₀	C3 _{3_b}	C3 _{2_b}	C3 _{1_b}	C3 _{0_b}
C3 ₃	C3 ₂	C3 ₁	C3 ₀	C2 ₃	C2 ₂	C2 ₁	C2 ₀
B7	B6	B5	B4	B3	B2	B1	B0

表 1.

注：_b 表示取反，如 C2_{3_b} 即 C2₃ 取反；C 表示控制位；B 表示备用位；

存取控制对控制块的控制如下表所示：

			密码 A	密码 A	存取控制	存取控制	密码 B	密码 B
C1	C2	C3	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	Never	KEYA B	never	never	Never
0	0	1	never	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；

数据块的存储控制如下表所示：

C1	C2	C3	Read	Write	Increment	decrement,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



版本列表

版本号	发布日期	页数	章节或图表	更改说明
1.0	2009.08	11		首次发布
2.0	2011.03	11		1. 修改笔误 2. 公司更名为“上海复旦微电子集团股份有限公司” 3. 北办地址门牌变更
2.1	2011.10	11		1. 修正电气参数及说明
3.0	2012.02	11		1. 修正部分电气参数
3.1	2013.09	11	销售及 服务网 点	1. 更新法律声明 2. 更新销售及 服务网 点

上海复旦微电子集团股份有限公司销售及服务中心

上海复旦微电子集团股份有限公司

地址：上海市国泰路 127 号 4 号楼

邮编：200433

电话：(86-021) 6565 5050

传真：(86-021) 6565 9115

上海复旦微电子（香港）股份有限公司

地址：香港九龙尖沙咀东嘉连威老道 98 号东海商业中心 5 楼 506 室

电话：(852) 2116 3288 2116 3338

传真：(852) 2116 0882

北京办事处

地址：北京市东城区东直门北小街青龙胡同 1 号歌华大厦 B 座 423 室

邮编：100007

电话：(86-10) 8418 6608

传真：(86-10) 8418 6211

深圳办事处

地址：深圳市华强北路 4002 号圣廷苑酒店世纪楼 1301 室

邮编：518028

电话：(86-0755) 8335 0911 8335 1011 8335 2011 8335 0611

传真：(86-0755) 8335 9011

台湾办事处

地址：台北市 114 内湖区内湖路一段 252 号 12 楼 1225 室

电话：(886-2) 7721 1889

传真：(886-2) 7722 3888

新加坡办事处

地址：237, Alexandra Road, #07-01, The Alexcier, Singapore 159929

电话：(65) 6472 3688

传真：(65) 6472 3669

北美办事处

地址：2490 W. Ray Road Suite#2 Chandler, AZ 85224 USA

电话：(480) 857-6500 ext 18

公司网址：<http://www.fmsh.com/>