Shanghai Fudan Microelectronics Group Company Limited

复旦微电子

FM11RF08S

8K bits EEPROM 非接触式逻辑加密卡芯片

技术手册

2022.09

目 录

1. 说明

本文档为 FM11RF08S 芯片技术手册。FM11RF08S 是复旦微电子公司开发的符合 ISO/IEC14443 协议逻辑加密卡芯片，具有较好的射频性能和射频兼容性，高可靠的数据存储。

2. 产品综述

2.1. 产品简介

FM11RF08S 是复旦微电子开发的一款非接触卡芯片，该芯片容量为 1K x 8 bits，符合 ISO14443 -A 标准，工作频率为 13.56MHz。

FM11RF08S 带三重防伪认证，内含加密控制和通讯逻辑电路，是具有保密功能和逻辑处理功能的多用途非接触射频卡芯片，可广泛应用于低成本的城市轨道交通、各类计费支付卡和数据采集系统等领域。

相对于 FM11RF08 芯片，在保证优良的卡机兼容性的前提下，提升了通信距离；在保证功能兼容性的前提下，通过弥补 M1 算法实现上的漏洞，创新性地提升了芯片的安全性和抗破解能力。

2.2. 产品特点

2.2.1. 射频接口

- 通讯协议：符合 ISO/IEC 14443-A
- 工作频率范围：13.56MHz
- 非接触的数据和能量传输（无需电源）
- 通讯波特率：106Kbit/s
- 操作距离不小于 100mm (和天线尺寸相关)
- 半双工通讯方式
- 加密算法符合 M1 标准
- 典型处理时间：＜100ms
- 支持加减法运算

2.2.2. EEPROM 存储器

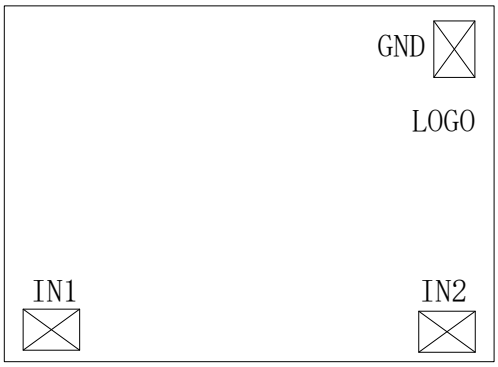
- 1024x8 bits EEPROM 存储单元
- 具有安全保护结构的 16 个独立的扇区，支持多种应用
- 对存储单元的访问权限可由用户根据自身的要求灵活定义
- 数据保存时间：大于 10 年
- 擦写次数：大于 20 万次

2.2.3. 安全特性

- 每颗芯片拥有唯一 UID 信息，UID 不可改写
- 三重安全认证
- 安全的数据通信
- 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
- 相对于旧版芯片，提升了抗破解能力

2.3. 引脚说明

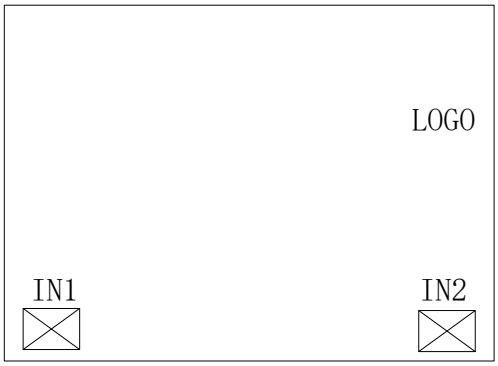
2.3.1. 减划晶圆



引脚序号	引脚名称	类型	引脚描述
1	IN1	输入/输出	天线接口 1
2	IN2	输入/输出	天线接口 2
3	GND	电源地	地

表 2-1 FM11RF08S 减划芯片 引脚说明

2.3.2. 凸点晶圆



引脚序号	引脚名称	类型	引脚描述
1	IN1	输入/输出	天线接口 1
2	IN2	输入/输出	天线接口 2

表 2-2 FM11RF08S 凸点芯片引脚说明

3. 功能描述

3.1. 总体描述

FM11RF08S 芯片由模拟射频电路、数字逻辑电路和存储器三部分组成，整体框图如下所示：

- **模拟射频电路：**完成数据解调和回发，为芯片提供稳定的电源和时钟。
- **数字逻辑电路：**完成协议处理，控制对 EEPROM 的读写。
- **非易失性存储器（EEPROM）：**提供高可靠的数据存储。

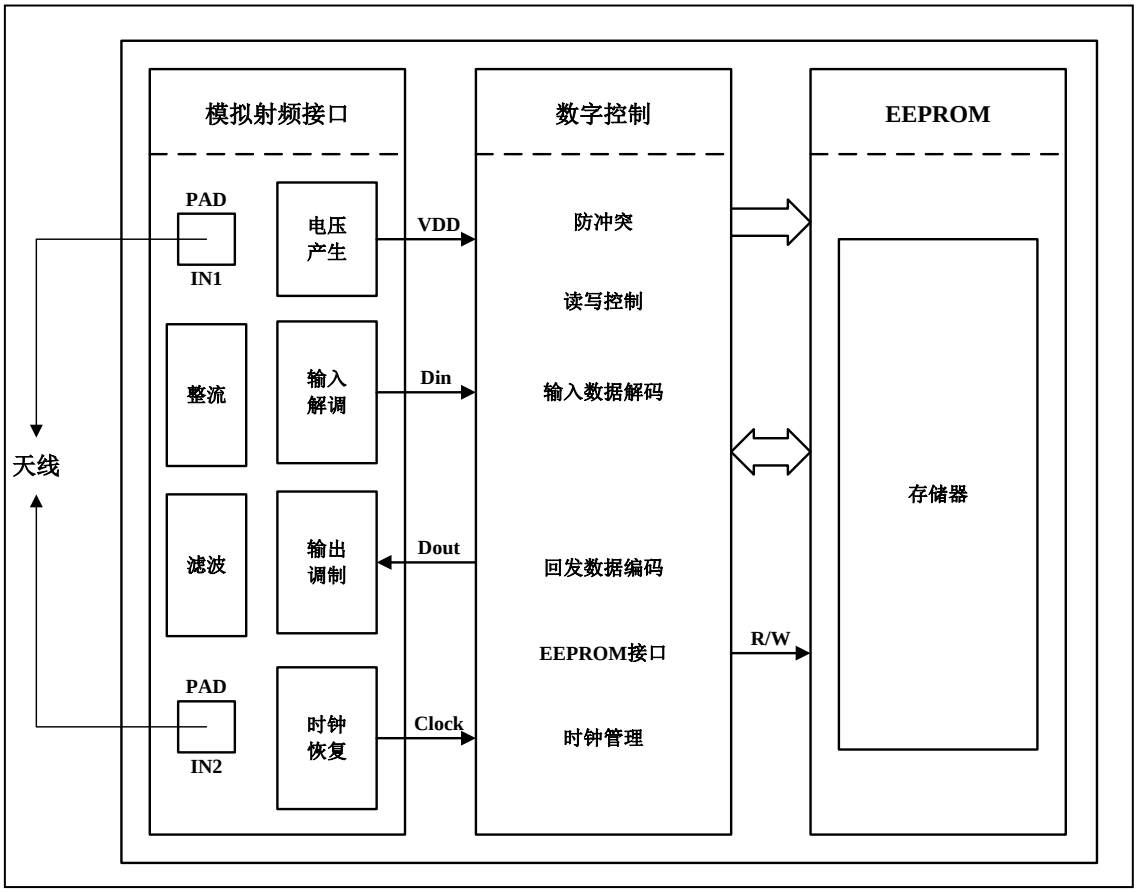


图 3-1 FM11RF08S 结构框图

3.2. 存储器

3.2.1. 存储分区和访问条件

FM11RF08S 芯片的 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。存储区的分区如下图所示：

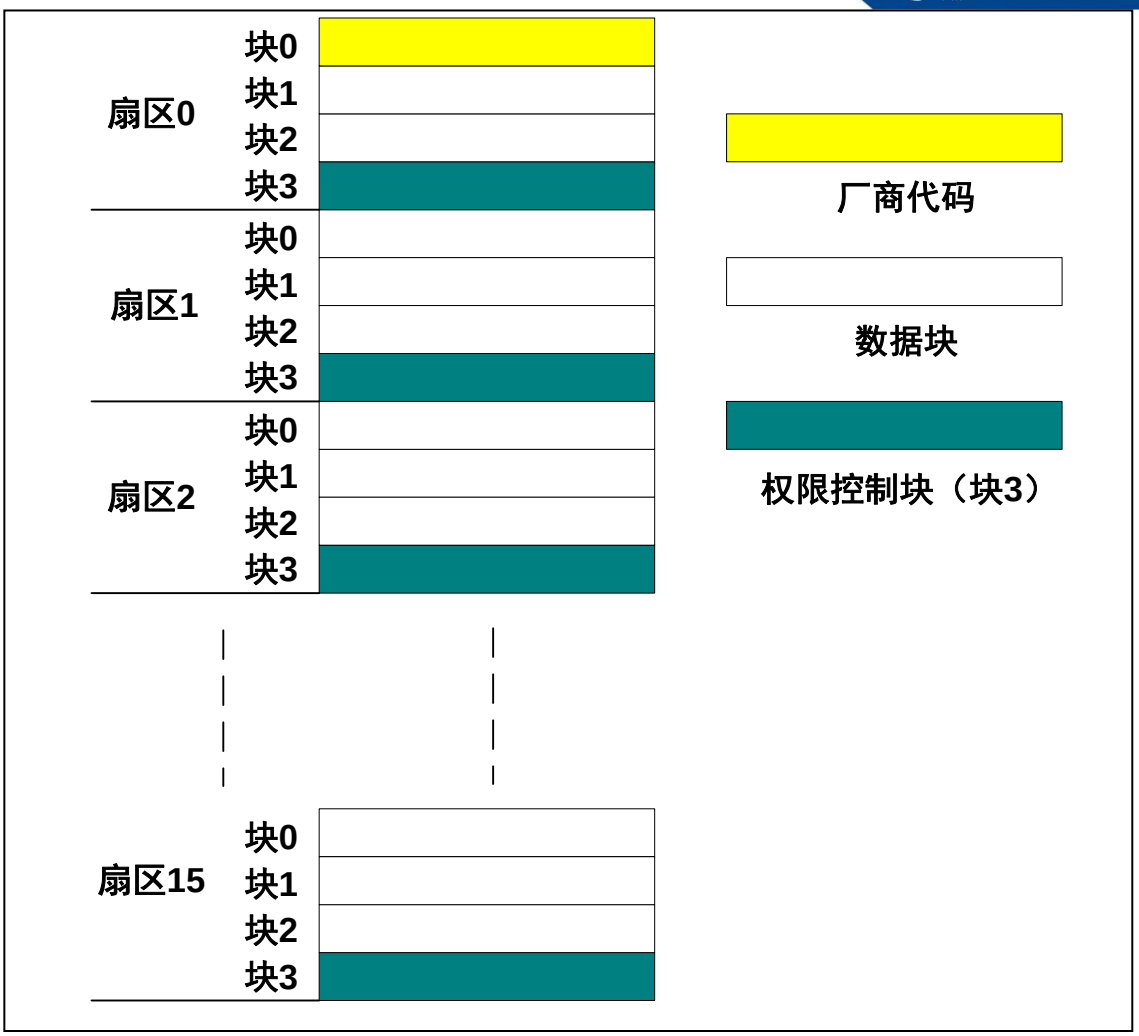


图 3-2 FM11RF08S 存储器分区图

每个扇区的块 3 包含了该扇区的密钥 A（6 个字节）、存取控制（4 个字节）和密钥 B（6 个字节），扇区 0 的块 0 是一个特殊的块，用于存放厂商的代码，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：

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
KeyA						Access Bits				KeyB					

图 3-3 FM11RF08S 存储器块 3 结构图

存储控制的结构如下：

	Bit7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Byte6	C2X3_b	C2X2_b	C2X1_b	C2X0_b	C1X3_b	C1X2_b	C1X1_b	C1X0_b
Byte7	C1X3	C1X2	C1X1	C1X0	C3X3_b	C3X2_b	C3X1_b	C3X0_b
Byte8	C3X3	C3X2	C3X1	C3X0	C2X3	C2X2	C2X1	C2X0
Byte9	BX7	BX6	BX5	BX4	BX3	BX2	BX1	BX0

注：

_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；

存取控制对块 3 的控制如下：(X=0-15)

			密钥 A	密钥 A	存取控制	存取控制	密钥 B	密钥 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	Never	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 表示密钥 A 或密钥 B；
Never 表示没有条件实现。

数据块的存储控制如下：(X=0-15 扇区、Y=每个扇区的 0-2 块)

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

3.2.2. 芯片唯一 UID

芯片 Sector0 block0 中存储了芯片独有的 7 字节序列号（UID）：

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
SN0~SN6							Chip Info								

Byte0~Byte6 为芯片制造商定义的芯片序列号。
根据 ISO14443-3 校验字节 BCC0 定义为 $CT \oplus SN0 \oplus SN1 \oplus SN2$，而 BCC1 定义为 $SN3 \oplus SN4 \oplus SN5 \oplus SN6$。
SN0 存储复旦微电子公司的制造商代码 1D。
UID 在芯片出厂前写入。芯片出厂后，UID 不可改写。

3.2.3. 芯片出厂配置

FM11RF08S 芯片 EEPROM 存储器的出厂配置数据如下：

Sector	Block	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	UID							Chip Info								
	1	00															
	2	00															
	3	FF						FF	07	80	69	FF					

Sector	Block	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	0	00															
	1	00															
	2	00															
	3	FF						FF	07	80	69	FF					

⋮

Sector	Block	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
15	0	00															
	1	00															
	2	00															
	3	FF						FF	07	80	69	FF					

3.3. 交易流程

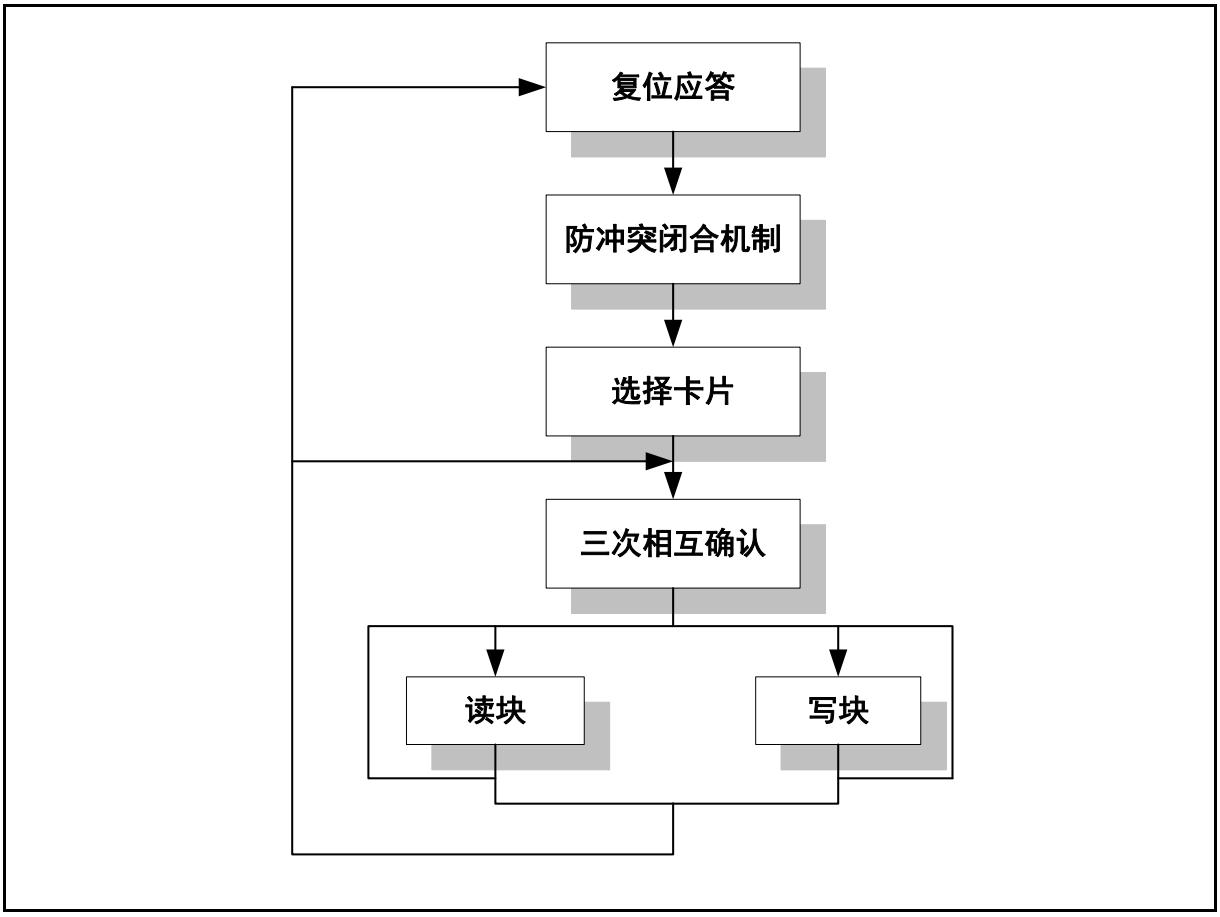


图 3-4 FM11RF08S 交易流程图

复位应答：FM11RF08S 芯片的通讯协议和通讯波特率遵从 ISO14443-A 规定，读写器和 FM11RF08S 芯片相互验证。当某张带有 FM11RF08S 的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 FM11RF08S 射频卡，即验证卡片的卡型。

防冲突闭合机制：当有多张 FM11RF08S 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。

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，并对该扇区的密钥进行校验，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钥校验）

读/写块：

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

3.4. 数据的完整性

在非接触通讯中，以下措施保证了读写器和芯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）

3.5. 安全性

FM11RF08S 支持安全鉴别和安全通信：

安全鉴别：读写前读写器和卡之间先进行三次相互认证过程，认证通过方能进行后续操作。

安全通信：卡的 EEPROM 中存储的数据，在空中传输时进行流加密，以密文的方式传输。

卡片中的密钥是受保护的、不可读的、只有知道密钥的用户才能修改它。

EEPROM 存储区可根据不同应用设定不同的密钥(一卡多用)。扇区的访问密钥分为KEYA 和KEYB 两组不同密钥，根据访问条件，在校验 KEYA 或 KEYB 之后才可以对相应的存储区进行访问。

3.6. FM11RF08S 芯片指令集

3.6.1. 指令列表

指令名称	指令代码（16 进制）
寻找处于空闲状态的卡	26
寻找所有操作区域内的卡	52
防冲突	93, 95
卡选择	93, 95
认证密钥 A	60
认证密钥 B	61
读块	30
写块	A0
加法	C1
减法	C0
恢复	C2
传输	B0

暂停	50

3.6.2. 指令说明

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。

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。

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。

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钥与卡内的密钥是否一致来获得。

读块指令：读出卡中某一块的 16 个字节。

写块指令：将数据写入卡中的某一块。

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。

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。

存储指令：将卡内数值块的内容读到卡内的寄存器。

传输指令：将卡内寄存器中的内容写入块中。

暂停指令：将卡片置于暂停状态。

4. 电气参数

4.1. 极限额定参数

参数	最小值	最大值	单位
存储温度	-55	+125	°C
输入电流（IN1 对 IN2；RMS）	-	30	mA
ESD （HBM） 【2】	-	±4	KV

表 4-1 FM11RF08S 极限额定参数【1】

*注【1】：如果外加条件超过“极限额定参数”的额定值，将会对芯片造成不可恢复的永久性破坏。

*注【2】： ESD 测试用 CDIP8 封装形式的芯片完成。

4.2. 推荐工作条件

符号	参数	条件	最小值	典型值	最大值	单位
T_A	工作温度	-	-40	+25	+85	°C
H_A	工作场强	-	1.5	-	7.5	A/M

表 4-2 FM11RF08S 推荐工作条件

4.3. 电参数

符号	参数	条件	最小值	典型值	最大值	单位
f_i	输入频率	【1】	13.553	13.56	13.567	MHz
C_i	输入谐振电容	IN1 和 IN2 之间【2】	13	15	17	pF

表 4-3 FM11RF08S 电参数

注【1】：频宽依据 ISM 频段规定

注【2】：使用 Agilent E5061B 在 13.56MHz 和 0.707V RMS 电压下测得

4.4. 存储器参数

符号	参数	条件	最小值	典型值	最大值	单位
tret	数据保存时间	环境温度小于 55 度	10	-	-	年
Nendu(W)	擦写次数	25 度	20	-	-	万次

表 4-4 FM11RF08S 存储器参数

5. 订货信息

器件代号	晶圆形式	规格说明
FM11RF08S-7B-WTB2	凸点晶圆	12 英吋凸点晶圆(120um 芯片厚度)。
FM11RF08S-7B-WTS5	减划晶圆	12 英吋减薄划片晶圆(150um 芯片厚度)。

FM 11RF 08 S -7B -XXX

公司名前缀

FM=上海复旦微电子集团股份有限公司

产品族

11RF= 符合 ISO/IEC 14443 协议的高频芯片

产品容量

08=8k bits EEPROM

版本

S：安全提升版本

UID

7B：7Byte UID

晶圆形式

WTS5= 减薄划片晶圆

WTB2= 凸点晶圆

版本信息

版本号	发布日期	页数	章节或图表	更改说明
1.0	2020.06	16		首次发布
1.1	2020.09	17		更新销售网点信息
1.2	2022.09	17		修正 UID 相关描述

上海复旦微电子集团股份有限公司销售及服务网点

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）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：深圳南山区西丽街道留仙大道创智云城 A7 座 2306-08
邮编：518000
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：47 Kallang Pudding Road, #08-06,The Crescent @ Kallang ,Singapore 349318
电话：(65) 6443 0860
传真：(65) 6443 1215

复旦微电子（美国）公司
地址：97 E Brokaw Road, Suite 320,San Jose,CA 95112
电话：(+1)408-335-6936

公司网址：http://www.fmsh.com/