非接触式 IC 卡性能简介（MF1 PHILIPS S50）

一、主要指标

- 容量为 8K 位 EEPROM
- 分为 16 个扇区，每个扇区为 4 块，每块 16 个字节,以块为存取单位
- 每个扇区有独立的一组密码及访问控制
- 每张卡有唯一序列号，为 32 位
- 具有防冲突机制，支持多卡操作
- 无电源，自带天线，内含加密控制逻辑和通讯逻辑电路
- 数据保存期为 10 年，可改写 10 万次，读无限次
- 工作温度：-20℃~50℃(湿度为 90%)
- 工作频率：13.56MHZ
- 通信速率：106 KBPS
- 读写距离：10 cm 以内（与读写器有关）

二、存储结构

1、M1 卡分为 16 个扇区，每个扇区由 4 块（块 0、块 1、块 2、块 3）组成，（我们也将 16 个扇区的 64 个块按绝对地址编号为 0~63，存贮结构如下图所示：

扇区 0	块 0		数据块	0
	块 1		数据块	1
	块 2		数据块	2
	块 3	密码 A 存取控制 密码 B	控制块	3
扇区 1	块 0		数据块	4
	块 1		数据块	5
	块 2		数据块	6
	块 3	密码 A 存取控制 密码 B	控制块	7
		⋮		
扇区 15	0		数据块	60
	1		数据块	61
	2		数据块	62
	3	密码 A 存取控制 密码 B	控制块	63

2、第 0 扇区的块 0（即绝对地址 0 块），它用于存放厂商代码，已经固化，不可更改。

3、每个扇区的块 0、块 1、块 2 为**数据块**，可用于存贮数据。

数据块可作两种应用：

★ 用作一般的数据保存，可以进行**读**、**写**操作。

★ 用作数据值，可以进行**初始化值、加值、减值、读值**操作。

4、每个扇区的块 3 为**控制块**，包括了密码 A、存取控制、密码 B。具体结构如下：

A0 A1 A2 A3 A4 A5	FF 07 80 69	B0 B1 B2 B3 B4 B5

密码 A（6 字节） 存取控制（4 字节） 密码 B（6 字节）

5、每个扇区的密码和存取控制都是独立的，可以根据实际需要设定各自的密码及存取控制。存取控制为 4 个字节，共 32 位，扇区中的每个块（包括数据块和控制块）的存取条件是由密码和存取控制共同决定的，在**存取控制**中每个块都有相应的**三个控制位**,定义如下：

块 0： C10 C20 C30
块 1： C11 C21 C31
块 2： C12 C22 C32
块 3： C13 C23 C33

三个控制位以正和反两种形式存在于存取控制字节中，决定了该块的访问权限（如进行减值操作必须验证 KEY A，进行加值操作必须验证 KEY B，等等）。三个控制位在存取控制字节中的位置，以块 0 为例：

对块 0 的控制：

	bit 7	6	5	4	3	2	1	0
字节 6				C20_b				C10_b
字节 7				C10				C30_b
字节 8				C30				C20
字节 9								

(注： C10_b 表示 C10 取反)

存取控制（4 字节，其中字节 9 为备用字节）结构如下所示：

	bit 7	6	5	4	3	2	1	0
字节 6	C23_b	C22_b	C21_b	C20_b	C13_b	C12_b	C11_b	C10_b
字节 7	C13	C12	C11	C10	C33_b	C32_b	C31_b	C30_b
字节 8	C33	C32	C31	C30	C23	C22	C21	C20
字节 9								

(注： _b 表示取反)

6、**数据块**（块 0、块 1、块 2）的存取控制如下：

控制位（X=0..2）			访 问 条 件 （对数据块 0、1、2）			
C1X	C2X	C3X	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

（KeyA|B 表示密码 A 或密码 B，Never 表示任何条件下不能实现）

例如：当块 0 的存取控制位 C10 C20 C30=1 0 0 时，验证密码 A 或密码 B 正确后可读；验证密码 B 正确后可写；不能进行加值、减值操作。

7、控制块块 3 的存取控制与数据块（块 0、1、2）不同，它的存取控制如下：

			密码 A		存取控制		密码 B	
C13	C23	C33	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

例如：当块 3 的存取控制位 C13 C23 C33=1 0 0 时，表示：

密码 A：不可读，验证 KEYA 或 KEYB 正确后，可写（更改）。

存取控制：验证 KEYA 或 KEYB 正确后，可读、可写。

密码 B：验证 KEYA 或 KEYB 正确后，可读、可写。

三、工作原理

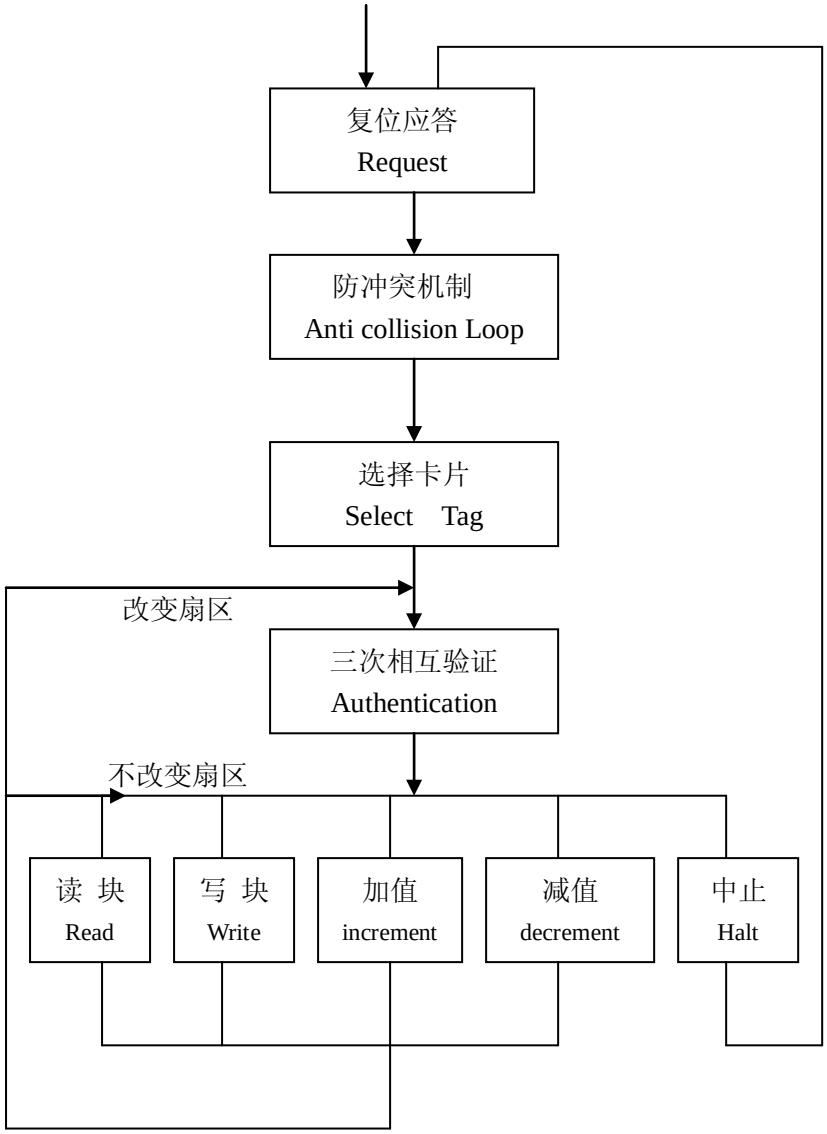
卡片的电气部分只由一个天线和 ASIC 组成。

天线：卡片的天线是只有几组绕线的线圈，很适于封装到 IS0 卡片中。

ASIC：卡片的 ASIC 由一个高速（106KB 波特率）的 RF 接口，一个控制单元和一个 8K 位 EEPROM 组成。

工作原理：读写器向 M1 卡发一组固定频率的电磁波，卡片内有一个 LC 串联谐振电路，其频率与讯写器发射的频率相同，在电磁波的激励下，LC 谐振电路产生共振，从而使电容内有了电荷，在这个电容的另一端，接有一个单向导通的电子泵，将电容内的电荷送到另一个电容内储存，当所积累的电荷达到 2V 时，此电容可做为电源为其它电路提供工作电压，将卡内数据发射出去或接取读写器的数据。

四、M1 射频卡与读写器的通讯



复位应答（Answer to request）

M1 射频卡的通讯协议和通讯波特率是定义好的，当有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 M1 射频卡，即验证卡片的卡型。

防冲突机制 (Anticollision Loop)

当有多张卡进入读写器操作范围时，防冲突机制会从其中选择一张进行操作，未选中的则处于空闲模式等待下一次选卡，该过程会返回被选卡的序列号。

选择卡片(Select Tag)

选择被选中的卡的序列号，并同时返回卡的容量代码。

三次互相确认(3 Pass Authentication)

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，在三次相互认证之后就可以通过加密流进行通讯。（在选择另一扇区时，则必须进行另一扇区密码校验。）

对数据块的操作

读（Read）：读一个块；

写（Write）：写一个块；

加（Increment）：对数值块进行加值；

减（Decrement）：对数值块进行减值；

存储（Restore）：将块 中的内容存到数据寄存器中；

传输（Transfer）：将数据寄存器中的内容写入块中；

中止（Halt）：将卡置于暂停工作状态；