一、概述

BL75R06SM 非接触加密存储卡芯片由射频通讯接口、安全控制单元和8K 位EEPROM 组成。读写距离10cm。主要适用于各种证件、电子钱包、自动收费系统和公共交通自动售检票系统等领域。该芯片支持ISO14443 TypeA 射频接口，支持PHILIPS 标准读卡机芯片。

二、产品特点

1 、RF 接口（ISO/IEC 14443 Type A）

- 芯片无需电池，数据和电源能量的提供通过无线传输
- 操作距离：最大达到 10 厘米（取决于天线）
- 操作频率： 13.56MHz
- 数据传输速率：106kbit/s
- 高数据完整性：16 位 CRC 校验，奇偶校验，位编码，位计数
- 典型交易时间：小于 100ms（包括备份管理时间）

2、 EEPROM

- EEPROM 存储容量为 8K 字节，分成 16 个扇区，每个扇区分成 4 个块，每块 16 个字节
- 每个存储块的访问条件可由用户自己定义
- 数据保持时间：最少 10 年
- 擦写次数：最少 10 万个周期

3、 安全

- 三重相互认证体制（ISO/IEC DIS9798-2）
- 通讯过程所有数据加密以防信号截取
- 每个扇区由相互独立的一套密码，支持一卡多用
- 每张卡的序列号唯一，传输密码保护
- 传输密码保护

三、芯片封装

根据客户需要可提供芯片模块或卡封装模式。

四、功能描述

1、BL75R06 原理图

BL75R06SM 芯片是非接触式 IC 卡芯片，芯片由射频通讯接口、数字逻辑控制模块（包括安全控制单元）、和 8K 字节的 EEPROM 存储器组成。能量和数据通过与 BL75R06 芯片直接连接的线圈组成的天线来传输，不需要任何外接部件。其原理如图 1。

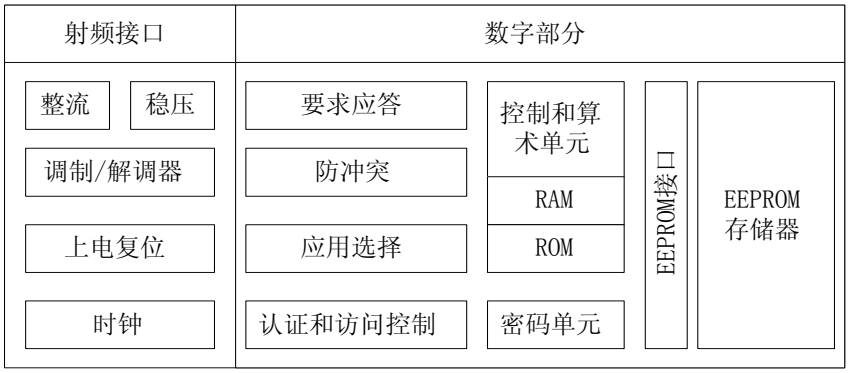


图 1 BL75R06 芯片的模块图

2、交易流程图

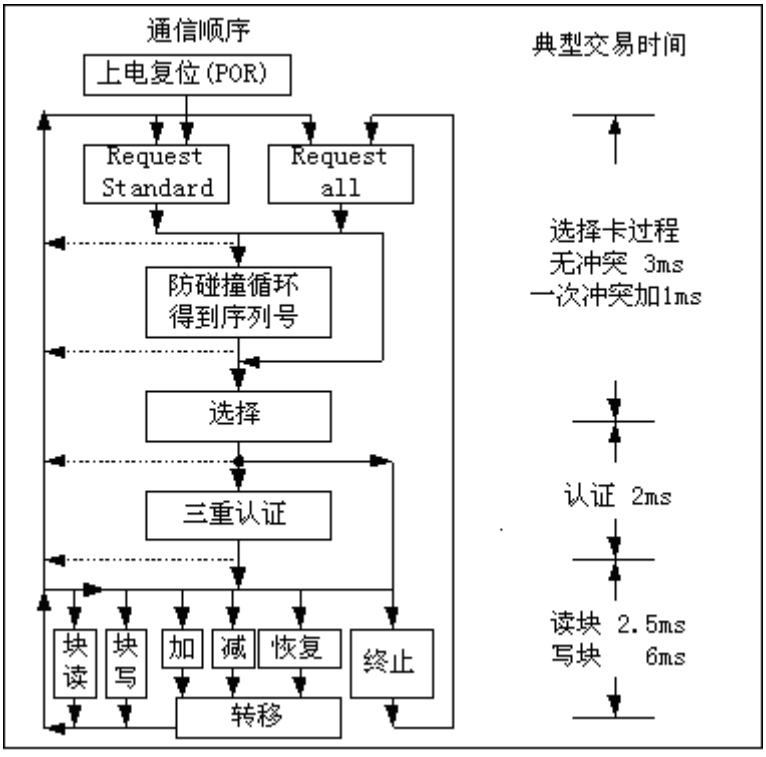


图 2 交易流程

2、通讯原理

BL75R06SM 芯片通过天线和 RWD 进行交互，由 RWD 发送命令，通过 BL75R06 内部的数字逻辑控制模块，根据要访问相应扇区的访问控制条件来决定命令的可操作性，并发送相应的信息或数据。

2.1 Request Standard/All 命令

智能卡在上电后，可以响应 Request 命令，该命令由读卡设备发送给射频场内所有的卡，卡发送请求响应（根据 ISO/IEC 14443A 协议的 ATQA ）。

2.2 防冲突循环

在防冲突循环过程中，读出卡的序列号。如果在读卡设备的操作范围内由几张卡，可以通过唯一的卡序列号来区别，并选中一张卡做为下一步操作的对象。没有被选中的卡返回到待命模式，等待下一个 Request 命令。

2.3 选卡

读卡设备发送选卡命令后，选择一张卡来认证和存储器相关操作。卡返回 ATS 代码（=08h）。该代码表示被选中卡的类型。

2.4 三重认证

卡选中后，读卡设备根据要访问的存储器位置，采用响应的密钥来进行三重相互认证过程。认证通过后，对存储器的操作都是加密的。

2.5 存储器操作

在认证后，可以进行如下操作：
读块
写块
减：块中的内容减去一个值，并把结果保存到一个临时的数据寄存器中。
加：块中的内容加去一个值，并把结果保存到一个临时的数据寄存器中。
恢复：块中的内容移到临时的数据寄存器中。
转移：将临时寄存器中的内容写到指定的值块中。

3、 数据完整性

在读卡设备和智能卡的无线通讯中，采用了如下的机制来保证数据传输的可靠性：

- 信息块的 16 位 CRC
- 每个字节带一个奇偶校验位

4、安全

为了提供高安全等级，采用了根据 ISO9798-2 协议的三重认证体制。

(1) 读卡设备确定要访问的扇区，然后选择 Key A 或 Key B
(2) 卡从扇区的 Trailer 块读出密钥和访问条件。然后发送一个随机数给读卡设备（第一重）
(3) 读卡设备用密钥和附加的输入计算卡的响应。然后发送一个响应和另一个随机数给卡（第二重）
(4) 卡验证读卡设备的响应，然后再计算一个响应给读卡设备（第三重）
(5) 读卡设备再验证卡的响应

再发送第一个随机数后，卡和读卡设备的通讯就都是加密了。

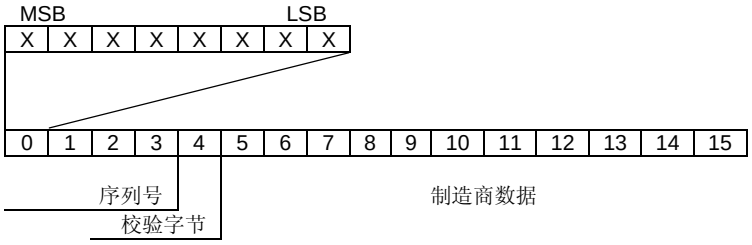
5、存储器结构

1024*8 bit 的 EEPROM 存储器由 16 个扇区构成，每个扇区有 4 块，每个块包含 16Bytes。在擦状态,EEPROM 单元读出逻辑“0”；在写状态,读出逻辑“1”。

		块内字节															
扇区	**块**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**描述**
15	3	密钥 A						存取位				密钥 B						扇区 Trailer 15
	2																	数据
	1																	数据
	0																	数据
14	3	密钥 A						存取位				密钥 B						扇区 Trailer 14
	2																	数据
	1																	数据
	0																	数据
…	…																	
…	…																	
…	…																	
1	3	密钥 A						存取位				密钥 B						扇区 Trailer 1
	2																	数据
	1																	数据
	0																	数据
0	3	密钥 A						存取位				密钥 B						扇区 Trailer 0
	2																	数据
	1																	数据
	0																	制造商块

5.1 制造商块

这是第一扇区（sector 0）的第一个数据块（block 0）。它包含 IC 制造商的数。由于安全和系统需要，当 IC 制造商在生产过程中编程以后，这个块是写保护的。



5.2 数据块

所有的扇区包含 3 个 16bytes 的块以储存数据（Sector 0 仅包含两个数据块和一个只读的制造商块）。数据块可以通过 access bits 进行配置，如下：

- 读/写块可以应用于非接触通行控制，或者
- 数值块可以应用于电子钱包，当附加的命令被提供，如直接控制存储的数值增加和减少的命令。

在任何的存储器操作以前，认证的命令必须执行，以便允许进一步的命令操作。

数值块提供执行电子钱包的功能（有效的命令：read，write，increment，decrement，restore，transfer）。数值块有一个固定的数据格式，允许错误侦测，修正和备份管理。数值块只可以在数值块格式下通过 write 操作创建。

- 数值：表示一个有正负号的 4-byte 数值。数值的最低位有效字节存储在最低位地址字节中。负数按标准的二进制补数的格式存储。因为数值完整性和安全性的原因，一个数值被存储三次，两次正常和一次取反。
- 地址：表示 1-byte 的地址，可用来保存块的存储地址，当执行强化的备份管理时。地址字节保存四次，两次取反和两次正常。当执行 increment, decrement, restore 和 transfer 操作时，地址保持不变。它仅可通过 write 命令改变。

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Value				Value				Value				Adr	$\overline{\text{Adr}}$	Adr	$\overline{\text{Adr}}$

5.3 扇区“Trailer”（BLOCK 3）

每一个扇区有一个扇区“Trailer”，包含：

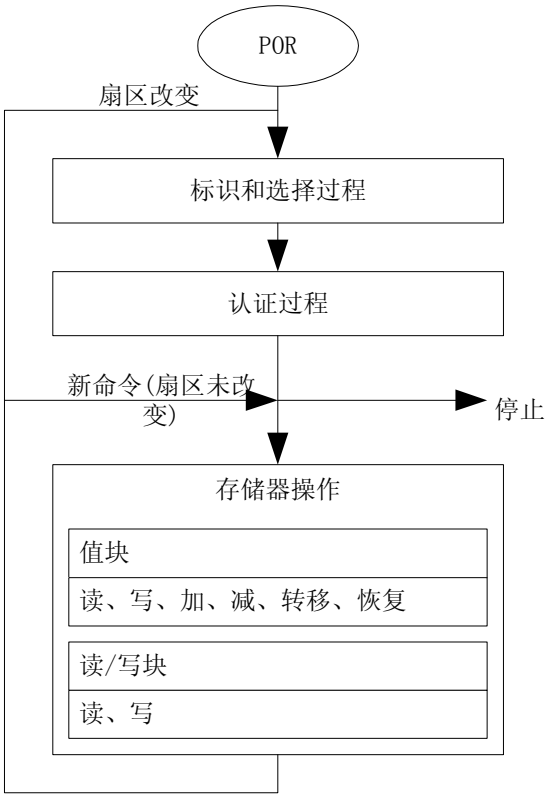
- 密钥 A 和 B（可选），在被读时返回逻辑“0”；
- 该扇区四个块的存取条件，存储在 6~9 字节中。Access bits 也指定数据块的类型（读/写或数值）。

如果密钥 B 不需要，block 3 的最后六个字节可以被用来作为数据字节。扇区“Trailer”的第九字节可被用来作为用户数据。因为这个字节支持与 byte 6，7 和 8 相同的存取权限。

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
密钥 A						存取位				密钥 B					

6、存储器访问

在任何存储操作可以被执行以前，卡必须被选择和认证，就像以前描述的那样。
对于一个可寻址块的可能的存储操作，依赖于使用的密钥，和保存在相关扇区尾记录中的存取条件。



存储器操作		
操作	描述	块类型有效
读	读块	读写、值和扇区 trailer
写	写块	读写、值和扇区 trailer
加	块中的内容加上一个值，并把结果保存到一个临时的数据寄存器中	值
减	块中的内容减去一个值，并把结果保存到一个临时的数据寄存器中	值
转移	将临时寄存器中的内容写到指定的值块中	值
恢复	块中的内容移到临时的数据寄存器中	值

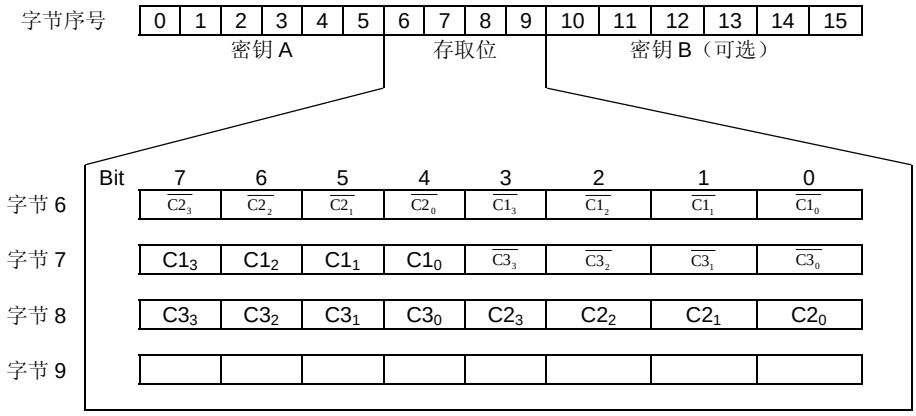
6.1 存取条件

每一个数据块和扇区尾记录的存取条件由 3bits 决定，保存正常和取反两种状态，在特定扇区的扇区尾记录中。Access bits 控制密钥 A 和 B 的存储器存取权限。存取条件可以被更改，倘若有人知道相关的密钥，并且当前存取条件允许这个操作。

NOTE：在以后的描述中，access bits 仅在正常情况下描述。

BL75R06 芯片的内部逻辑保证，只有在通过认证后命令才执行存储器相关指令，否则永远不执行。

存取位	有效命令		块	描述
$C1_3C2_3C3_3$	读、写	→	3	扇区 trailer
$C1_2C2_2C3_2$	读、写、加、减、转移、恢复	→	2	数据块
$C1_1C2_1C3_1$	读、写、加、减、转移、恢复	→	1	数据块
$C1_0C2_0C3_0$	读、写、加、减、转移、恢复	→	0	数据块



NOTE：对于每一次的存储器存取，内部逻辑检查存取条件的格式。如果检测到格式错误，整个扇区将无可挽回的封闭。

6.2 扇区“Trailer”的存取条件

根据扇区尾记录的 access bits，对密钥和 access bits 的读/写控制被指定为“never”，“key A”，“key B”或“key A|B”（key A 或 key B）。在芯片交货时，扇区尾记录的存取条件和 key A 是预先确定的，作为传送器配置，新的卡必须用 key A 认证。因为 access bits 也可以自我封闭，所以在操作卡时必须特别小心。

存取位			存取条件						说明
			密钥 A		存取位		密钥 B		
C1	C2	C3	读	写	读	写	读	写	
0	0	0	不可	密钥 A	密钥 A	不可	密钥 A	密钥 A	密钥 B 可读
0	1	0	不可	不可	密钥 A	不可	密钥 A	不可	密钥 B 可读
1	0	0	不可	密钥 B	密钥 A|B	不可	不可	密钥 B	
1	1	0	不可	不可	密钥 A|B	不可	不可	不可	
0	0	1	不可	密钥 A	密钥 A	密钥 A	密钥 A	密钥 A	密钥 B 可读,传输配置
0	1	1	不可	密钥 B	密钥 A|B	密钥 B	不可	密钥 B	
1	0	1	不可	不可	密钥 A|B	密钥 B	不可	不可	
1	1	1	不可	不可	密钥 A|B	不可	不可	不可	

NOTE：在灰色标记的行中， key B 是可读的，因此可以被用来作为数据。

6.3 数据块的存取条件

根据数据块（blocks0~2）的 access bits，读/写控制被指定为“never”，“key A”，“key B”或“key A|B”（key A 或 key B）。相关的 access bits 的设置，指定了应用的范围和相应支持的命令。

- 读/写块：允许读和写的操作。
- 数值块：允许附加命令的操作：increment，decrement，transfer 和 restore。在一种情况下（001），对于非可充值卡，只有 read 和 decrement 命令可以被执行。在另一种情况（110），充值可以通过使用 key B 来实现。
- 制造商块：只读的条件不受 access bits 设置的影响。
- 密钥管理：在传送器配置下，key A 必须被用来作认证 [1]。

存取位			存取条件				应用
C1	C2	C3	读	写	加	减、转移、恢复	
0	0	0	密钥 A|B[1]	密钥 A|B[1]	密钥 A|B[1]	密钥 A|B[1]	传输配置
0	1	0	密钥 A|B[1]	不可	不可	不可	读/写块
1	0	0	密钥 A|B[1]	密钥 B[1]	不可	不可	读/写块
1	1	0	密钥 A|B[1]	密钥 B[1]	密钥 B[1]	密钥 A|B[1]	值块
0	0	1	密钥 A|B[1]	不可	不可	密钥 A|B[1]	值块
0	1	1	密钥 B[1]	密钥 B[1]	不可	不可	读/写块
1	0	1	密钥 B[1]	不可	不可	不可	读/写块
1	1	1	不可	不可	不可	不可	读/写块

[1] 如果 Key B 可以在相应的扇区尾记录中被读出，它不能被用来认证（上表中所有的灰色行）。

结论：如果读卡机试图使用 key B 来认证任何一个使用灰色存取条件的扇区中的块，卡都将拒绝执行认证后的任何存储器操作。