Chip Card & Security ICs

256-Byte 逻辑加密存储卡芯片 FT4442

特点

- 低电压、低功耗：
  - FT4442: V_{CC} = 2.0V 到 5.5V
- 256× 8 bit 的 EEPROM 数据存储区结构
- 32 × 1 bit 保护存储区
- 字节寻址
- 前 32 个地址不可逆字节写保护
- 双线通信协议，触点定义和串行接口符合 ISO 7816 标准（同步传输）
- 数据输出时指示处理结束
- 单字节擦写编程时间 2.5ms
- 4,000V 的 ESD 保护
- 至少 10 万次的擦写周期
- 至少 10 年的数据保存期
- 数据存储区仅在输入正确的 3 字节可编程密码（PSC）后才可擦写

概述

FT4442 是辉芒微电子自行开发的 2Kbit 的接触式 IC 卡芯片。采用特殊的 CMOS 工艺制造实现的低功耗、低电压 (2.0V to 5.5V) 性能使其具有广泛的应用领域。

管脚描述

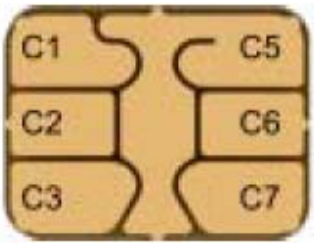

图 1: M3.2 触点模式

触点定义及功能描述

触点	符号	功能
C1	VCC	工作电压
C2	RST	复位
C3	CLK	时钟
C5	GND	接地
C6	N.C.	无效
C7	I/O	输入/输出(开漏)

表 1

功能描述

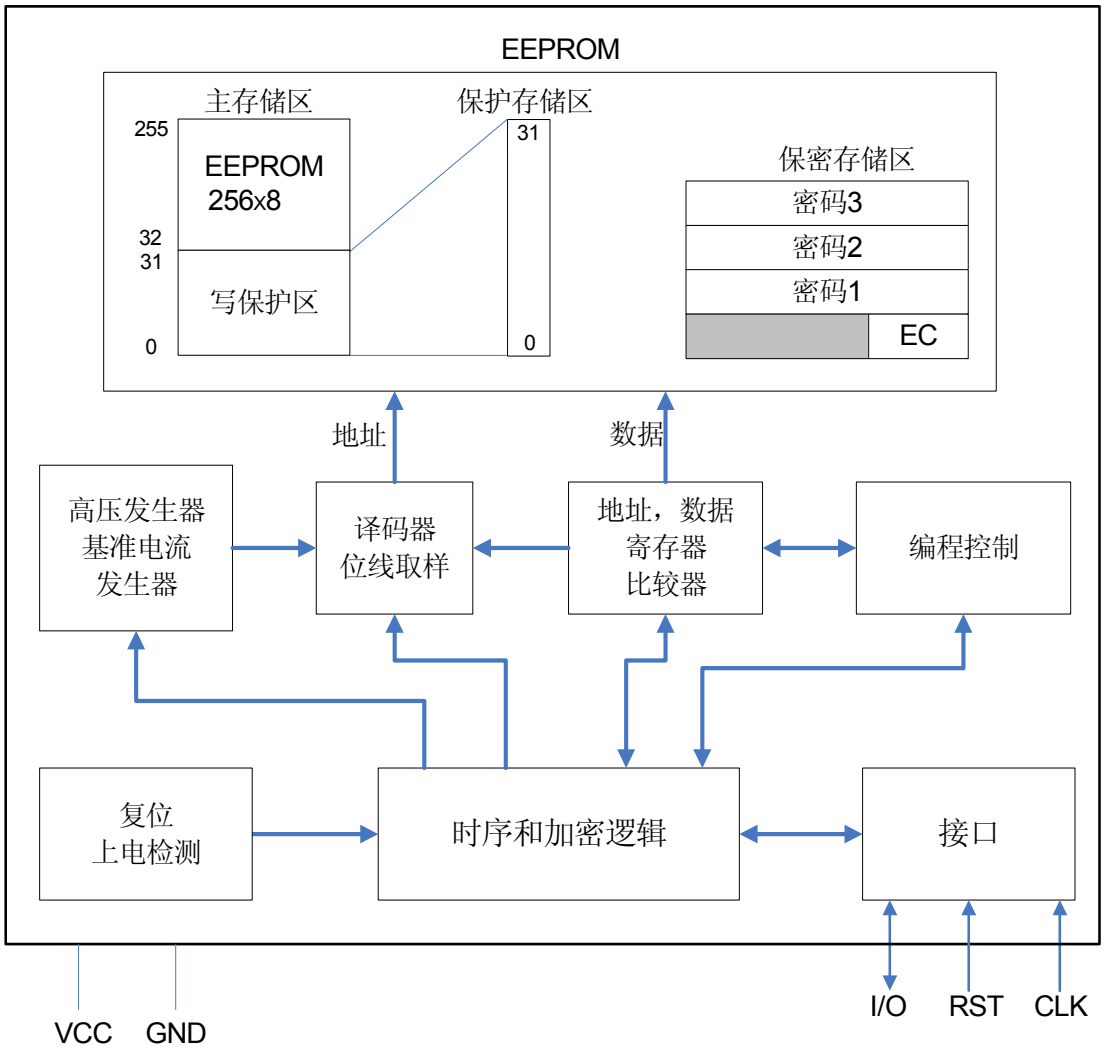

图 2：原理框图

存储区结构

FT4442 内部具有一个 256 字节的 EEPROM 主存储区（数据存储区）和一个 32 位的 PROM 保护存储区。主存储区按字节擦写。擦除时，数据字节的 8 位都置为逻辑“1”，写入时，被操作的字节根据输入数据按位改写成逻辑“0”。 通常，一次数据的改写过程由一次擦除和一次写入过程组成。EEPROM 是否进行改写取决于主存储区数据字节与新数据字节的内容。如果指定字节的 8 位没有一位需要 0 至 1 的翻转, 就跳过擦除操作。反之，如果不需要 1 至 0 的翻转, 就省却写入操作。写和擦除的工作至少需要 2.5ms。

主存储区起始 32 个字节可以通过写保护存储区中对应的位不可逆转地防止被改写。该地址范围内的每个数据字节与保护存储区中的一比特相对应，而且与主存贮器具有相同的地址。保护位一旦写入就不能再擦除。

除上述功能外 FT4442 还提供一个控制对存储区进行擦除/写入的密码逻辑。为此，FT4442 设定了一个包含 3 字节密码和 1 字节出错计数器 EC 的保密存储区。3 字节的密码称为可编程密码 (PSC)。 加电后，除这些密码外，整个存储区只能被读取。只有在校验数据和密码比较相同后才能对芯片进行写操作 ，直到芯片掉电。3 次密码比较失败后，出错计数器将封锁所有后续尝试，禁止对存储区的擦、写操作。

传输协议

传输协议为接口设备 IFD 和 IC 之间的两线连接协议。协议类型标识为"S=A"。I/O 上的所有数据交换由 CLK 的下降沿触发。

传输协议由 4 个模式组成：

- 复位与响应复位
- 命令模式
- 数据输出模式
- 数据处理模式

注意： I/O 引脚开漏输出，因而需要上拉电阻来实现逻辑“1”。

A) 复位与响应复位

响应复位按 ISO7816-3 标准产生。操作期间任何时候都可以给出复位信号。复位时，地址计数器由一时钟脉冲置到零；当 RST 从 H 态置成 L 态时，第一个数据位(LSB)输出到 I/O。通过此后连续的 31 个时钟脉冲，可读出前 4 个 EEPROM 地址单元中的内容。第 33 个时钟脉冲将 I/O 置成 H 态。在响应复位期间，忽略所有启动和停止条件。

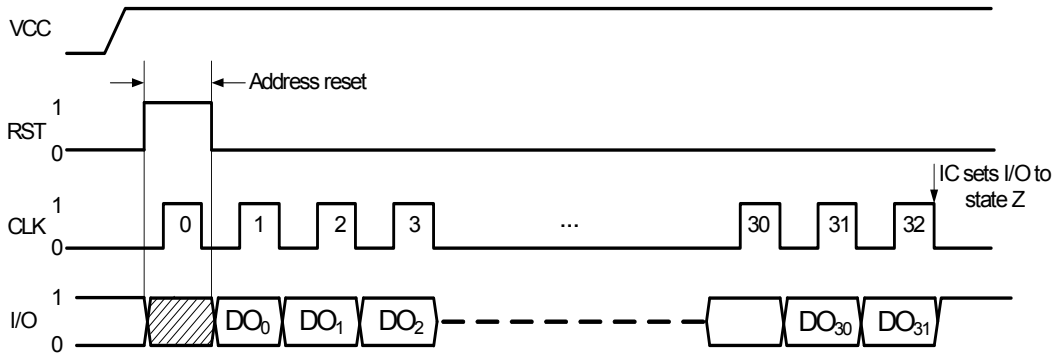

图3：复位和响应复位

B) 操作模式

命令模式

响应复位后，IC 等待命令的输入。每条命令从一启动条件开始，包括 3 个字节长的命令体及其后的一个附加时钟脉冲，最后由停止条件结束。

- 起始条件：CLK 处于 H 态期间，I/O 线上的下降沿
- 结束条件：CLK 处于 H 态期间，I/O 线上的上升沿

接收命令后，IC 有两种可能的模式：

- 读操作时的数据输出模式
- 写入和删除操作时的处理模式

数据输出模式

在此模式下，IC将数据发送至IFD。在CLK上的第一个下降沿后，I/O上第一个数据位有效。在最后一个数据位后，为使I/O成为H态并使IC准备好接收新命令，需要一个额外的时钟脉冲。在此模式期间，任何起始和停止条件均不起作用。

数据处理模式e

在此模式下，IC进行内部处理。在CLK的第一个下降沿后变成L态的I/O线恢复H态前，必须向IC连续提供时钟信号。在此模式期间任何起始和停止条件均不起作用。

注意： 在此模式期间RST置为低。如果 在CLK为低电平时将RST置为高，任何当前操作都将中止。

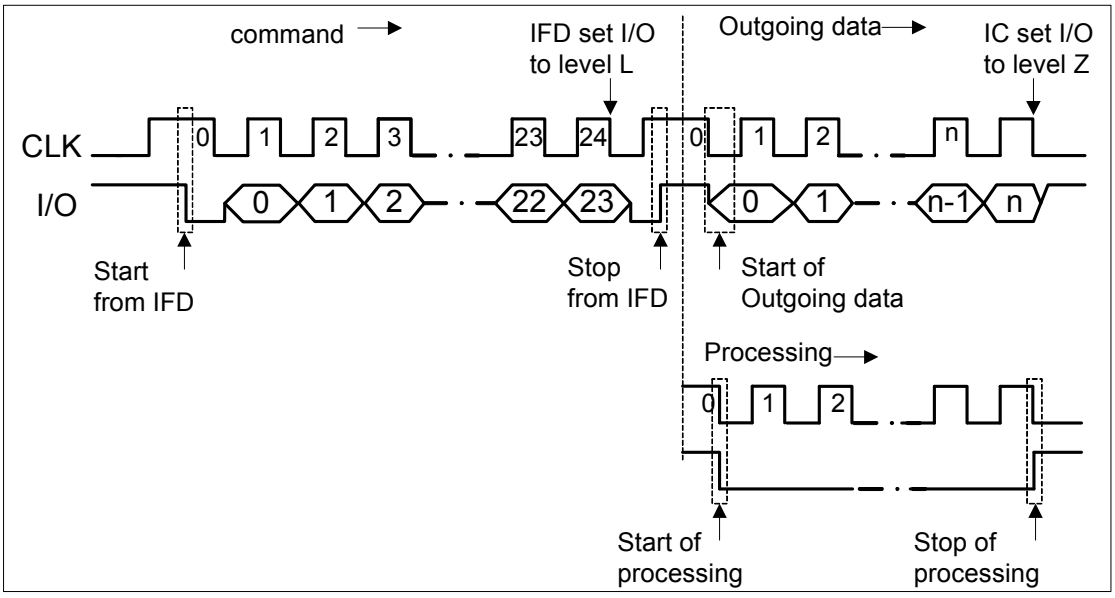

图 4：操作模式

C) 命令

命令格式

每个命令包含 3 个字节：命令码、地址码、数据码。由命令码的最低位开始传输。

MSB			指令				LSB	MSB			地址				LSB	MSB			数据				LSB
B7	B6	B5	B4	B3	B2	B1	B0	A7	A6	A5	A4	A3	A2	A1	A0	D7	D6	D5	D4	D3	D2	D1	D0

表2

主存储区河保护存储区的 4 条命令如表 1 所示。安全存储区的 3 条命令，见表 2。

字节1 指令								字节2 地址	字节3 数据	操作	模式
B7	B6	B5	B4	B3	B2	B1	B0	A7-A0	D7-D0		
0	0	1	1	0	0	0	0	地址	无效	读主存	数据输出
0	0	1	1	1	0	0	0	地址	数据	更新主存	数据处理
0	0	1	1	0	1	0	0	无效	无效	读保护存储区	数据输出
0	0	1	1	1	1	0	0	地址	数据	写保护存储区	数据处理

表 3

字节 1 指令								字节 2 地址	字节 3 数据	操作	模式
B7	B6	B5	B4	B3	B2	B1	B0	A7-A0	D7-D0		
0	0	1	1	0	0	0	1	无效	无效	读保密存储区	数据输出
0	0	1	1	1	0	0	1	地址	数据	更新保密存储区	数据处理
0	0	1	1	0	0	1	1	地址	数据	密码验证	数据处理

表 4

读主存储区

该命令读出从所给出的字节地址(N)开始到存储区最后一个地址的主存储区中数据内容(LSB先读出)。在此命令输入后，IFD必须提供足够的时钟脉冲。脉冲数m = (256 – N) × 8 + 1。对主存的读操作总是可以执行的。

读保护存储区

此命令在连续32个脉冲驱动下将保护位传送到输出端，利用一附加脉冲可使I/O置成“H”状态。保护存储区总是可读的。

更新主存储区

此命令将要传送的数据字节写入指定地址的EEPROM 字节。根据新旧数据，处理模式期间将执行下述操作序列中一种：

- 擦除和写入 (5 ms) 对应 m = 255 个时钟脉冲
- 不擦除直接写入 (2.5 ms) 对应 m = 124 个时钟脉冲
- 只擦除不写入 (2.5 ms) 对应 m = 124 个时钟脉冲

(所有数值在50 kHz 时钟下计算得到)

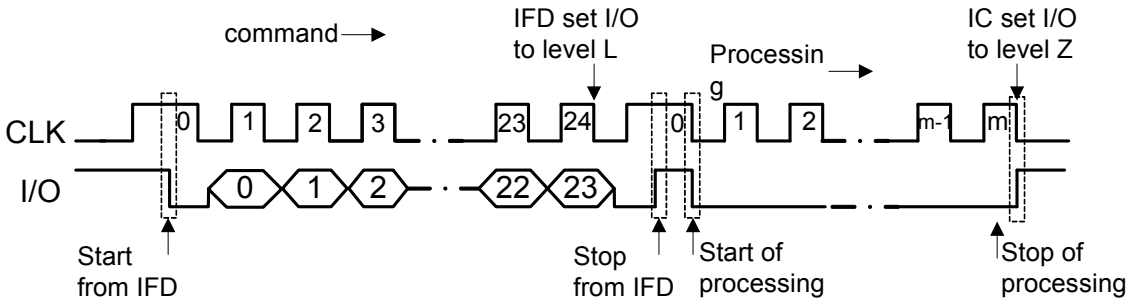

图 5：读主存储区

写保护存储区

此命令的执行包括一个输入数据字节与EEPROM中指定字节的比较过程，如果指定字节的数据与指令输入数据一致，就执行写保护位操作，使此数据信息成为不可改变的。如果两者数据不同，写保护位的操作就将被禁止。执行时间和所需脉冲同“更新主存储区”。

读保密存储区

类似于保护存储区的读命令，此命令读出保密存储区的4 个字节。数据输出模式期间的时钟脉冲数为32。通过一个附加脉冲，I/O 被置成H态。如无预先成功的PSC认证，参考数据字节（密码）的输出就被禁止的，这意味着I/O仍然处在“L"”态。

更新保密存储区

关于参考数据字节，只有在成功地认证了PSC后，此命令才能执行，否则，只有出错计数器（地址0）的各位可以有从“1”写成“0”的更新。执行时间和所需的时钟脉冲与上述“更新主存储区”的相同。

比较认证数据

此命令只能与出错计数器的一次更新步骤组合使用（见PSC验证），该命令将输入的一个认证数据字节和对应的参考数据字节进行比较，对此过程来说，处理模式期间的时钟脉冲是必需的（至少2 个脉冲）。

D) PSC 验证

FT4442要求在改写数据前必须先验证存储在保密存储区中的可编程密码（PSC）。

以下流程必须严格按所述顺序进行，任何改变都可能导致失败，以致擦除/写入均无法进行。只要此过程没有成功结束，出错计数器(EC)的各位只能从“1”变“0”，而不能进行擦除。

首先，错误计数器的某一位必须通过一条更新命令(UPDATE)写成“0”（见图6）。然后，从参考数据的字节1 开始执行三次“比较认证命令”。整个过程的成功结束可以通过能够擦除非自动擦除的出错计数器来辨别。至此，只要不掉电，就可以对整个存储区域进行写入(擦除)操作。只要错误计数器还有1位，上述整个过程就可以重新进行。在密码比较通过后，参考数据可以像EEPROM 中的任何其它信息一样被改变。

下表给出了PSC验证必需的几条命令。命令的顺序不可更改。

命令	指令	地址	数据	备注
	B7…B0	A7…A0	D7…D0	
读保密存储区	31_H	无效	无效	检查错误计数器 EC
更新保密存储区	39_H	00_H	数据	将 EC 某一位写为“0”
验证密码	33_H	01_H	数据	验证密码字节 1
验证密码	33_H	02_H	数据	验证密码字节 2
验证密码	33_H	03_H	数据	验证密码字节 3
更新保密存储区	39_H	00_H	FF_H	擦除错误计数器 EC
读保密存储区	31_H	无效	无效	检查错误计数器

PSC 根据与用户之间独立协议进行编码。这样，要改变数据就必须知道此代码。

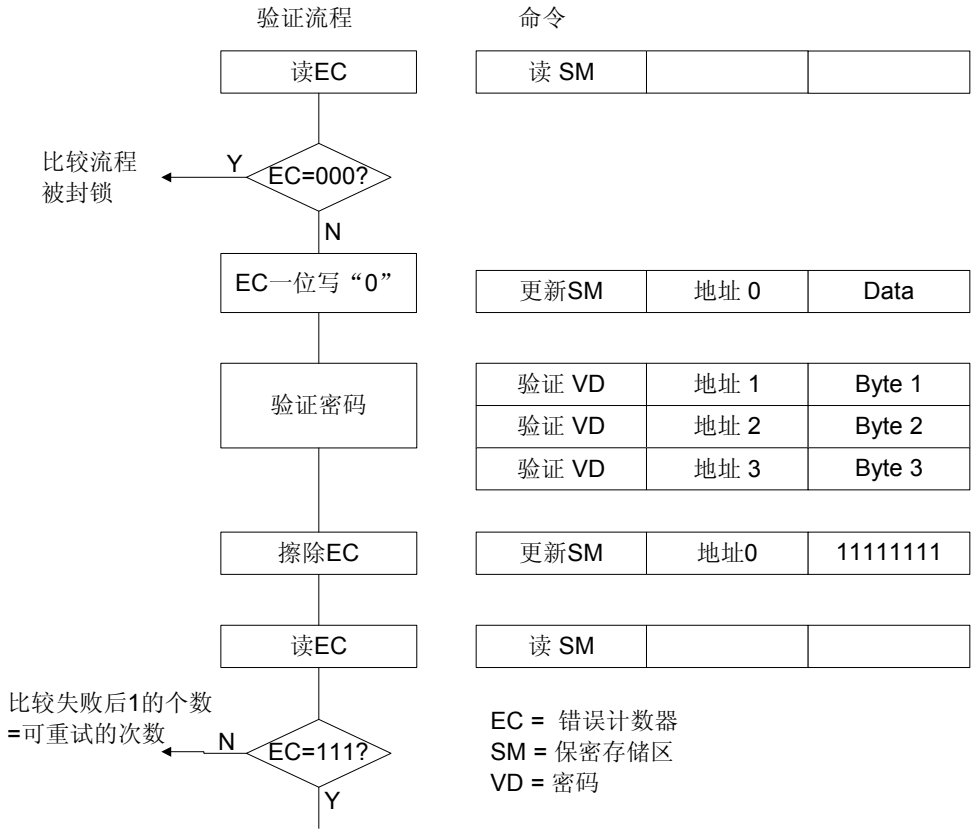

图5：PSC验证流程

E) 复位模式

复位与复位应答(见 A))

上电复位

在将VCC与操作电压接通后，I/O处于H态。在可以改变数据之前，必须执行一次对任意地址或响应复位的读操作。

F) 中止

如果CLK处于L态时将RST置H，任何操作都将被中止，同时I/O被置成H态。为触发一次已定义的有效复位，需要tRES = 5 us的最短间隔。在中止后，IC等待进一步的操作。

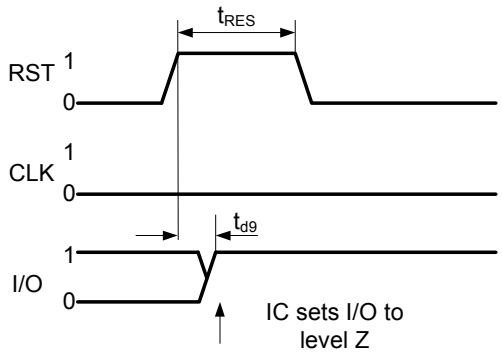

图7：中止

G) 故障

故障表现：假使出现下列故障，IC在最后8个时钟脉冲后将I/O置为H态，可能的故障是：

- 密码比较失败
- 错误的命令
- 不正确的命令时钟数
- 对已被写保护的字节进行擦除/写入操作
- 保护存储区中某一位的重复擦除

操作信息

存储区映射

地址 (十进制)	主存储区	保护存储区	保密存储区
255	数据字节 255(D7…D0)		
. . .	. . .		
32	数据字节 32(D7…D0)		
31	数据字节 31(D7…D0)	保护位 31(D31)	
. . .	. . .	. . .	
3	数据字节 3(D7…D0)	保护位 3(D3)	密码字节 3(D7…D0)
2	数据字节 2(D7…D0)	保护位 2 (D2)	密码字节 2(D7…D0)
1	数据字节 1(D7…D0)	保护位 1(D1)	密码字节 1(D7…D0)
0	数据字节 0(D7…D0)	保护位 0(D0)	EC(0,0,0,0,0,D2,D1,D0)

第 0 到 31 的数据字节可以通过写相应的 0 到 31 个 bit 的保护存储区获得写保护功能。FT4442 仅在密码验证成功后才可改写数据。读主存储区以及保护存储区总是可执行的。

电气参数

A) 绝对最大额定值

参数	符号	限定值		单位
		最小值	最大值	
工作电压	V_{CC}	-0.3	6.0	V
输入电压	V_1	-0.3	6.0	V
保存温度	T_{stg}	-40	125	℃
功耗	P_{tot}		70	mW

注意： 超出上述最大额定值可能造成器件永久性的损伤。 这里仅仅给出了临界额定值，而在临界限额定值或手册中其它部分所述的临界值下的功能操作情况未给出。在绝对最大额定值条件下长时间工作，可能导致器件可靠性的问题，比如EEPROM的数据保存期以及可重复擦写的次数。

B) 操作范围

参数	符号	限定值			单位	测试条件
		最小值	典型值	最大值		
工作电压	V_{CC}	2.0		5.5	V	-
工作电流	I_{CC}		3	10	mA	V_{CC} =5V
工作温度	T_A	0		70	℃	-

C) 直流参数

参数	符号	限定值			单位	测试条件
		最小值	典型值	最大值		
输入高电平(I/O,CLK,RST)	V_{IH}	3.5		V_{CC}	V	-
输入低电平 (I/O,CLK,RST)	V_{IL}	0		0.8	V	-
高电平输入电流(I/O,CLK,RST)	I_{IH}			50	μA	V_{IH} =5V
低电平输出电流(I/O)	I_{OL}	1			mA	V_{OL} =0.4V, 开漏
高电平输出电流(I/O)	I_{OH}			50	μA	V_{OH}=5V, 开漏
输入电容	C_1			10	pF	

D) 交流参数

以时间为单位的交流参数如下表所示。V_{IHmin} 和V_{ILmax} 作为参考电平用于测量信号的变化时刻。

参数	符号	限定值			单位	测试条件
		最小	典型	最大		
CLK 频率	CLK	7		50	KHz	-
CLK 高电平时间	t_H	9		0.8	μs	-
CLK 低电平时间	t_L	9			μs	
CLK 上升	t_R			1	μs	
CLK 下降	t_F			1	μs	
启动条件的保持时间	t_{d1}	4			μs	
RST 到输出有效时间	t_{d2}			2.5	μs	
停止条件建立时间	t_{d3}	4			μs	
RST 的建立时间	t_{d4}	4			μs	
数据保持时间	t_{d5}	1			μs	
响应复位	t_{d6}	20			μs	
数据建立时间	t_{d7}	1			μs	
启动条件的建立时间		4			μs	
中止信号最短时间	t_{RES}	5			μs	
中止信号延迟时间		2.5				
擦除时间	t_{ER}	2.5			ms	f_{CLK} = 50KHz
写入时间		2.5			ms	f_{CLK} = 50KHz
新启动条件前的时间间隔	t_{BUF}	10			μs	

