



SQ7131/SQ7133/SQ7135

简要中文产品规格书 V1.7

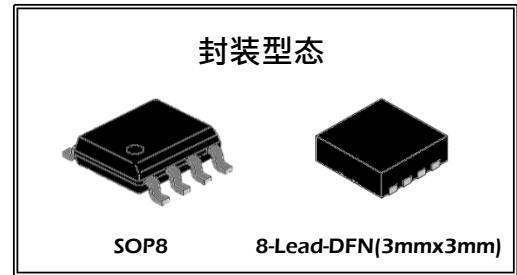
SQ7131/SQ7133/SQ7135 ,低功耗安全加密芯片, ECC-256/384, ECDSA,ECDH, AES-128/AES-256, SHA-256,TRNG

◆ **工作范围**

- 工作电压: 2.0V ~ 5.5V
- 工作温度: -40℃ ~ 85℃

◆ **通讯接口**

- SQ7131支持I2C界面(Max: 1MHz)
- SQ7133支持SPI界面(Max: 10MHz@MODE3)
- SQ7135支持SWI (Single Wire Interface)界面(230.4Kbps)



◆ **安全特性**

- NIST标准之非对称式硬件加速器，用於数字签名生成、验证、密钥合意协定
 - NIST P256 /P384椭圆曲线
 - ECDSA: FIPS 186-4椭圆曲线数字签名
 - ECDH: FIPS SP800-56A密钥合意协议(Key Agreement)
- NIST标准之硬件对称式加密算法
 - FIPS 180-4 SHA-256 & FIPS 198-1 HMAC哈希算法
 - FIPS-197 AES-128/256 : 加密/解密, Galois Field Multiply for GCM
- 支持网络密钥管理
 - TLS 1.2 & 1.3 PRF/HKDF计算
 - ECDHE 密鑰交換協定(密鑰生成、密鑰合意協議)
- NIST ESV认证并符合CMVP FIPS 140-3标准; NIST CAVP认证: DRBG, AES, SHA2, ECDSA and HMAC
- SESIP & PSA Level 3认证
- STQC Level 2认证
- 高质量TRNG设计，兼容SP800-22标准
- 防篡改(Anti-Tamper)保护，对企图入侵进行监测并做出反应
- 简单/差分功率分析攻击防御设计(SPA/DPA, Simple/Differential Power Analysis Attact Countermeasure)
- 独立内部时钟、防止外部Glitch攻击
- 128位唯一标识符 (UID)

◆ **安全存储**

- 芯片加扰加密技术
- 安全存储区-密钥、X.509 压缩证书、数据
- 大容量User Data : 5.6KB

◆ **应用**

- | | |
|----------------------|---------|
| ■ 安全传输TLS1.2与TLS 1.3 | ■ 配件认证 |
| ■ AIoT 装置安全认证 | ■ 端到端加密 |
| ■ 安全启动/安全远程更新 | ■ 防盗版 |

目录

1. 产品简介.....	4
2. 引脚配置.....	5
2.1 SQ7131 引脚配置/说明.....	5
2.2 SQ7133 引脚配置/说明	6
2.3 SQ7135 引脚配置/说明.....	7
3. 电气特性.....	8
3.1 极限参数.....	8
3.2 工作条件.....	9
3.2.1 工作条件.....	9
3.2.2 I/O 特性.....	9
3.3 DC 特性	10
3.4 上电复位电气特性.....	11
3.5 BROR 电气特性	12
3.6 AC 特性.....	13
3.6.1 运行模式时序特性.....	13
3.6.2 I2C 特性.....	14
3.6.3 SPI 特性.....	15
3.6.4 SWI 特性.....	17
3.7 EEPROM 特性.....	19
附录 A. 封装信息.....	20
附录 B. 订购信息.....	22
附录 C. 产品型号信息	23
修改纪录	24

1.产品简介

SQ713x 支持多种硬件加密加速器：高质量 TRNG（真随机数发生器）、SHA-256、非对称加密 ECC-384/ECC-256 和对称加密 AES-128/AES-256。它还具有用于 ECC 和 AES 密钥存储的安全存储。

本装置适用于构建高安全性应用，如物联网对称/非对称认证、认证、TLS1.2/1.3 安全连接、安全启动、安全 OTA 和固件保护等。

ECC 和 AES 密钥的安全存储：

Key Type	SQ713x	Note
AES Key (AES-128/256)	12	Slot 8~19
ECC Private Key – 256	7	Slot 1~7
ECC Private Key – 384	2	Slot 20,21
ECC Public Key – 256	4	Slot 24,26~28
ECC Public Key – 384	4	Slot 30,32~34

表 1-1 AES 及 ECC 密钥存储器槽(KEY SLOTS)概要

2. 引脚配置

2.1 SQ7131 引脚配置/说明

产品型号 : SQ7131SP008C00R

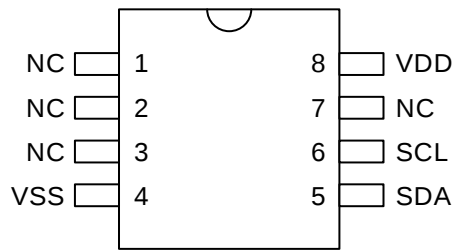


图 2-1 SQ7131 SOP8 封装型态引脚配置

产品型号 : SQ7131N3008C00R

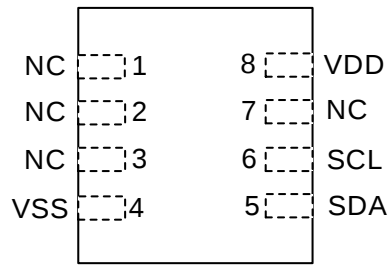


图 2-2 SQ7131 8-Lead DFN 封装型态引脚配置

引脚编号	引脚名称与端口/选择功能	输入输出 I/O类型	叙述
1	NC	-	不连接
2	NC	-	不连接
3	NC	-	不连接
4	VSS	GND	接地
5	SDA	I/O	I2C ,串行数据输入/输出引脚
6	SCL	I	I2C , 串行时钟输入引脚
7	NC	-	不连接
8	VDD	电源	VDD 电源输入

2.2 SQ7133 引脚配置/说明

产品型号 : SQ7133SP008S00R

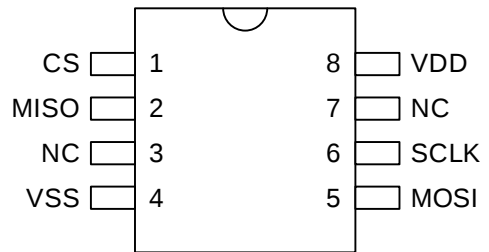


图 2-3 SQ7133 SOP8 封装型态引脚配置

产品型号 : SQ7133N3008S00R

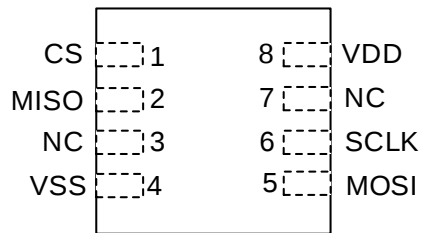


图 2-4 SQ7133 8-Lead DFN 封装型态引脚配置

引脚编号	引脚名称与端口/选择功能	输入输出 I/O类型	叙述
1	CS	I	SPI, 芯片选择引脚
2	MISO	O	SPI, 主设备输入/从设备输出引脚
3	NC	-	不连接
4	VSS	GND	接地
5	MOSI	I	SPI, 主设备输出/从设备输入引脚
6	SCLK	I	SPI, 串行时钟输入引脚
7	NC	-	不连接
8	VDD	电源	VDD 电源输入

2.3 SQ7135 引脚配置/说明

产品型号 : SQ7135SP008W00R

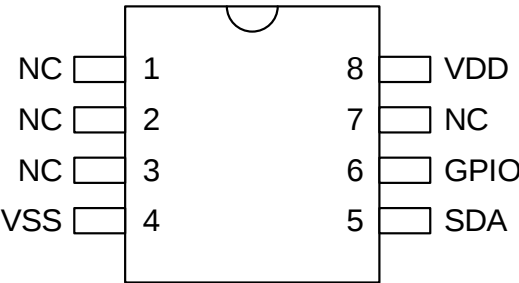


图 2-5 SQ7135 SOP8 封装型态引脚配置

产品型号 : SQ7135N3008W00R

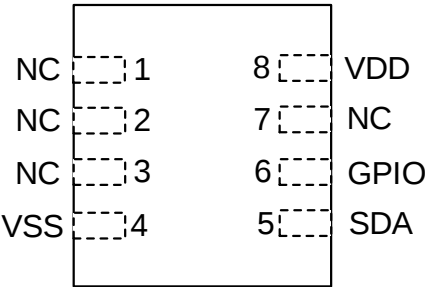


图 2-6 SQ7135 8-Lead DFN 封装型态引脚配置

引脚编号	引脚名称与端口/选择功能	输入输出 I/O类型	叙述
1	NC	-	不连接
2	NC	-	不连接
3	NC	-	不连接
4	VSS	GND	接地
5	SDA	I/O	SWI ,串行数据输入/输出引脚
6	GPIO	I/O	通用输入/输出引脚
7	NC	-	不连接
8	VDD	电源	VDD 电源输入

3. 电气特性

3.1 极限参数

单片机操作时切勿超过以下任一项极限参数值。即使仅是极短时间，也可能造成单片机损坏或性能衰退，严重者可能导致起火或爆炸、造成伤害。因此，请确保采用本单片机设计开发之产品 或系统不超过以下极 限参数值。

(V_{SS} = 0V)

参数	符号	引脚	极限参数	单位
供电电压范围	V _{DD}	-	-0.3 to 6.0	V
输入电压范围	V _{IN}	All I/O pins	-0.3 to VDD+0.3	V
最大输出电流(总和)	I _{OL}	All I/O pins	100	mA
保存温度范围	T _{STG}	-	-50 to 125	°C

3.2 工作条件

以下定义出当装置于「电压及温度最大/最小值」运行时其电气特性。「标准」条件是在「室温 25℃及标准工作电压 VDD=3.3V」下测定而得。若有不同于以上定义或是更详细的工作条件，会于各表格中的「测试条件」字段中注明该条件。

3.2.1 工作条件

参数	符号	最小	标准	最大	单位
工作电压	V _{DD}	2.0	3.3	5.5	V
工作温度	T _a	-40	25	85	℃

3.2.2 I/O 特性

参数	符号	条件	最小	标准	最大	单位
Input Low Voltage	V _{IL}	VDD=5V, temperature=25 °C	0		0.3 VDD	V
Input High Voltage	V _{IH}	VDD=5V, temperature=25 °C	0.7 VDD		VDD	V
Output Low Voltage	V _{OL}	VDD=5V, temperature=25 °C IOL= 3 mA	0		0.1 VDD	V
Output High Voltage	V _{OH}	VDD=5V, temperature=25 °C IOH= -3 mA	0.9VDD		VDD	V

3.3 DC 特性

参数	符号	最小	标准	最大	单位
运行模式(Operation Mode)下的操作电流 (Note)	IDD_N1	-	3.7	-	mA
深眠模式(Deep Sleep Mode)下的操作电流	IDD_DS	-	0.3	-	uA
工作模式下的供电电流 (非 ECC 命令执行期间)	IDD_N2		4.3		mA
工作模式下的供电电流 (执行 ECC 命令期间)	IDD_N3		7		mA

Note :此状态为等待 Command 期间。

3.4 上电复位电气特性

Ta=-40~85℃					
符号	叙述	最小	标准	最大	单位
tPPW	上电复位最小脉宽 Power-on reset minimum pulse width	1	-	-	ms
tPWUP	上电复位后到装置 ready 时间 Warming-up time after a reset is clear and device ready	-	4	-	ms
tVDD	上电时间 Power supply rise time	0.5	-	5	ms

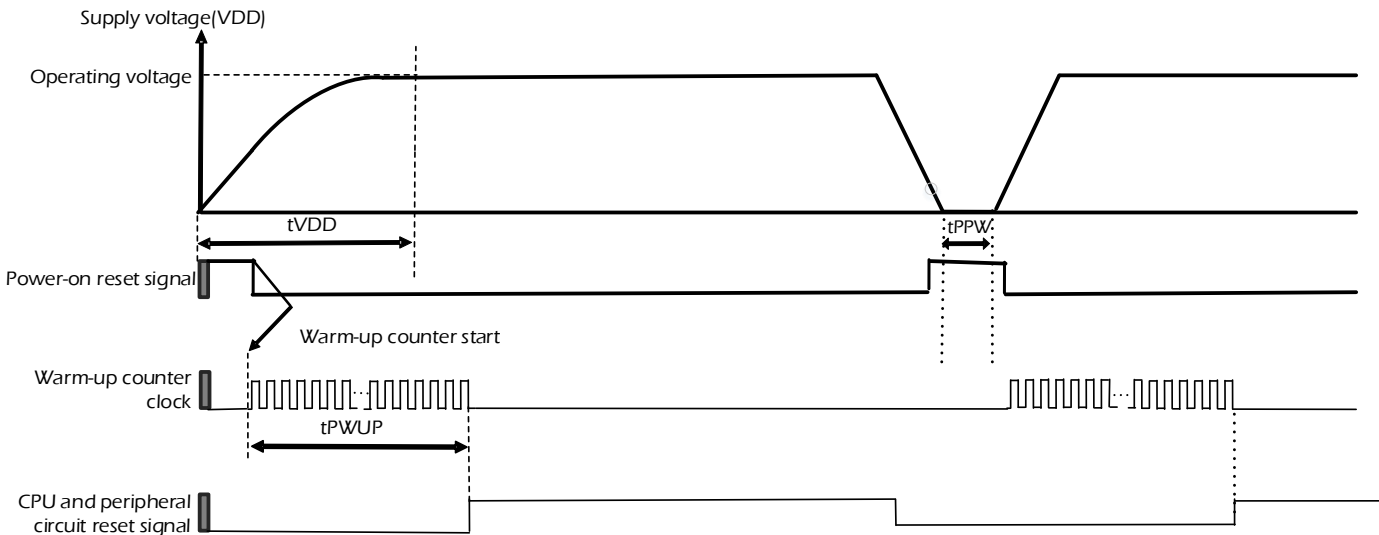


图 3-1 上电复位时序图

Note：当系统下电时，电压需低到 0V 再重新上电，才能确保重新上电后的 IC 动作正常。

3.5 BROR 电气特性

Ta=-40~85℃						
参数	符号	测试条件	最小	标准	最大	单位
BROR 检测电压	VBROR_Falling	VDD fall time > tVDD (tVDD 请参考 <u>Ch3.4 Power-on Reset Characteristics</u>)	1.85	1.90	1.95	V

3.6 AC 特性

3.6.1 运行模式时序特性

参数	符号	最小	标准	最大	单位
上电后就绪时间 Power-Up Ready Time	T _{PU_RDY}	-	9.5	-	ms
上电后就绪时间，准备接收指令 Power-Up Ready Time – Ready for Command	T _{CMD_RDY}	-	18.5	-	ms
Standby 时间，进入 deep sleep 模式 Standby Time, Entering the deep sleep mode	T _{STB}	-	20	-	us
唤醒就绪时间，deep sleep 模式 Wake-Up Ready Time, deep sleep mode	T _{WDS_RDY}	-	2.4	-	ms

注：“标准”值基于 25℃ 室温，“Sleep”命令将改变此值。

3.6.2 I2C 特性

参数	符号	最小	最大	单位
SCL 时钟频率(Clock Frequency)	f_{SCL}	-	1	MHz
重启条件保持时间 (Hold Time Repeated START Condition) 第一个时钟脉冲产生跟随在此时间之后发生。	$t_{HD;STA}$	0.45	-	us
SCL 时钟低电平周期 (Low Period of SCL Clock)	t_{LOW}	0.65	-	us
SCL 时钟高电平周期 (High Period of SCL Clock)	t_{HIGH}	0.35	-	us
重启条件设置时间 (Setup Time for a Repeated START Condition)	$t_{SU;STA}$	0.35	-	us
数据保持时间 (Data Hold Time)	$t_{HD;DAT}$	-	0.5	us
数据设置时间 (Data Setup Time)	$t_{SU;DAT}$	0.1	-	us
SDA 与 SCL 上升时间 (Rise Time of both SDA and SCL)	t_r	20	300	ns
SDA 与 SCL 下降时间 (Fall Time of both SDA and SCL)	t_f	20	300	ns
停止条件设置时间 (Setup Time of STOP Condition)	$t_{SU;STO}$	0.6	-	us
停止条件与开始条件间的总线自由时间 (Bus Free Time between a STOP and START Condition)	t_{BUF}	1.3	-	us
每条总线之电容负载 (Capacitive Load for each Bus Line)	C_b	-	400	pF

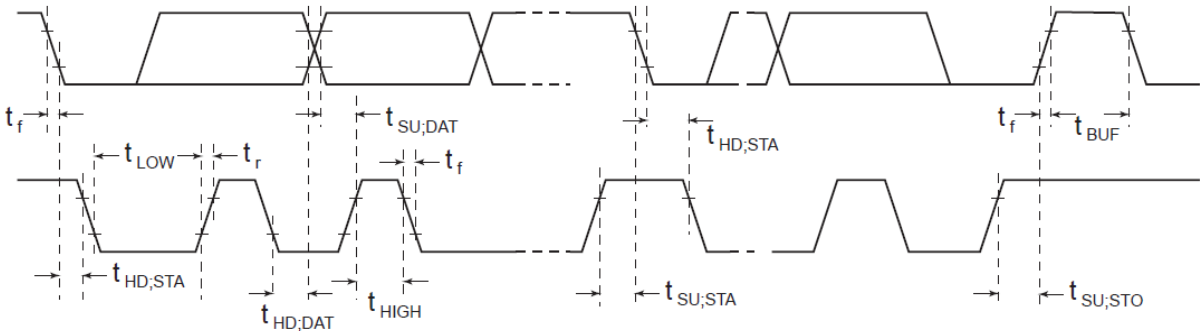


图 3-2 I2C 时序图

3.6.3 SPI 特性

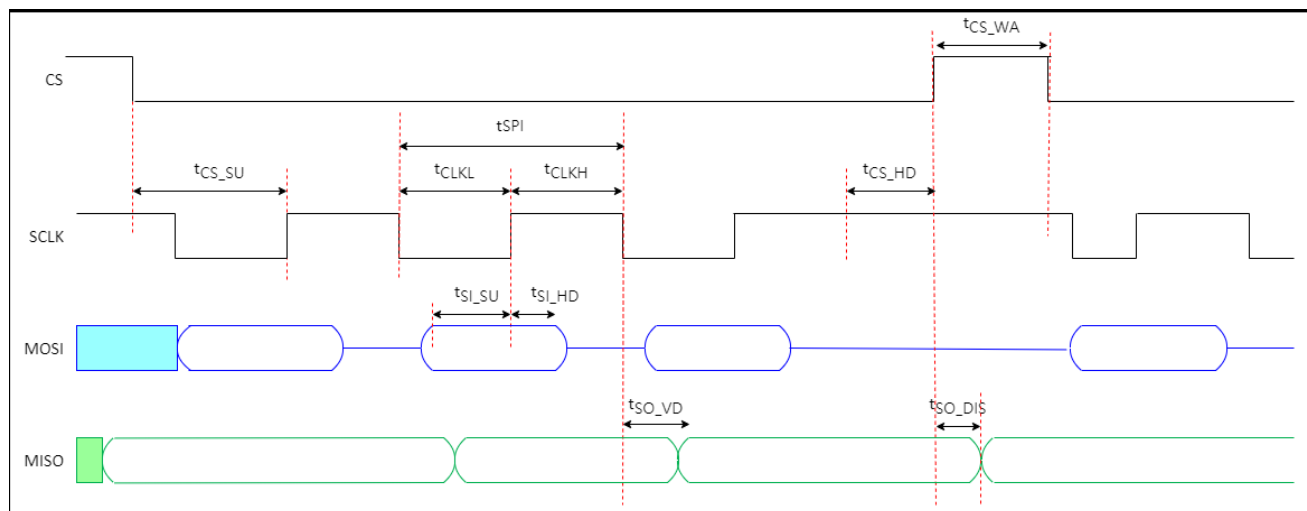


图 3-3 SPI 时序图

参数	符号	最小	最大	单位
SPI 频率 SPI Frequency	fSPI	-		
(VDD=2.7V~5.5V, ≤55°C)			10	MHz
(VDD=2.7V~5.5V, >55°C)			8	MHz
(VDD=2.0V~2.7V)			5	MHz
SPI 周期 SPI Period	tSPI	1/fSPI	-	ns
SCLK 高电平周期 High period of the SCLK pin	tCLKH	0.4 tSPI	-	ns
SCLK 低电平周期 Low period of the SCLK pin	tCLKL	0.4 tSPI	-	ns
从 SPICS 有效到第一个边沿的时间 From SPICS active to first sample edge	tCS_SU	2.0 tSPI	-	ns
从最后一个 SCLK 边沿到 SPICS 无效的时间 From last SCLK shift edge to SPICS inactive	tCS_HD	2.0 tSPI	-	ns
SPI 传输时间 Time between SPI transaction	tCS_WA	3.0 tSPI	-	ns
输入数据设置时间 ¹ Data Input Setup Time	tSI_SU	25	-	ns
输入数据保持时间 ¹ Data Input Hold time	tSI_HD	10	-	ns
输出数据有效时间 ¹ Data Output Valid Time	tSO_VD	-	40	ns

参数	符号	最小	最大	单位
输出数据禁止时间 ¹ Data Output Disable Time	tSO_DIS	-	25	ns

注 1：这些参数是特性参数，但未在生产中测试。

3.6.4 SWI 特性

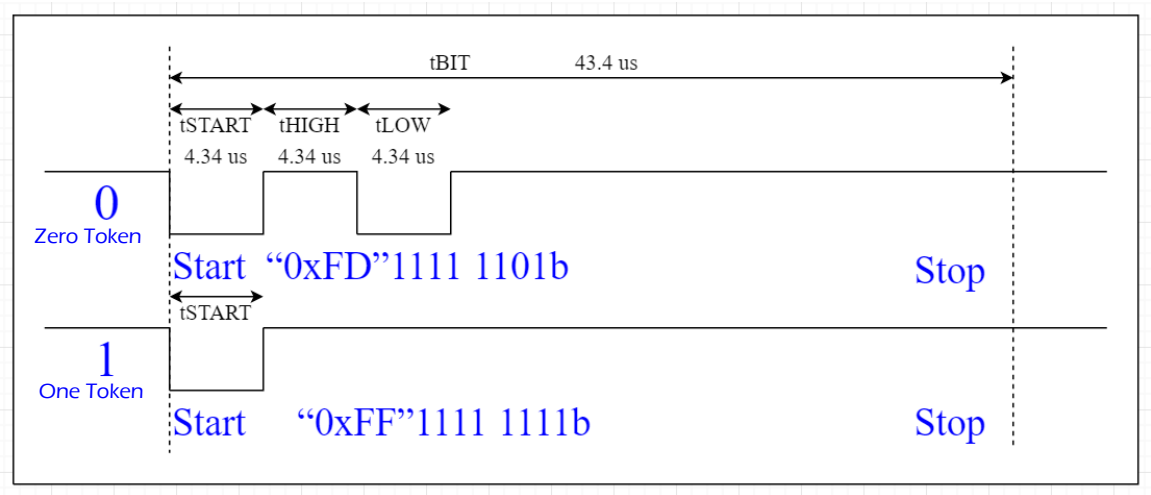


图 3-4 SWI 时序图@230.4k (标准)

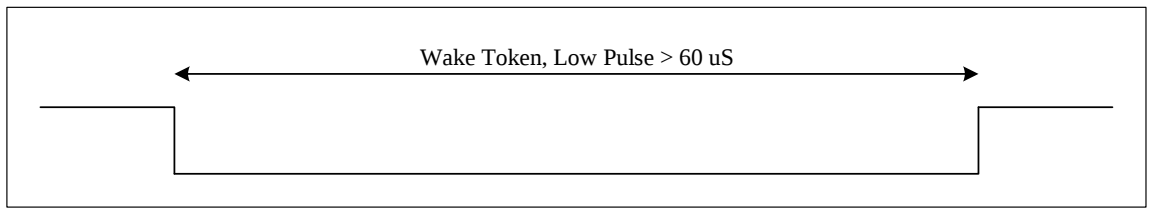


图 3-5 SWI 唤醒时序图

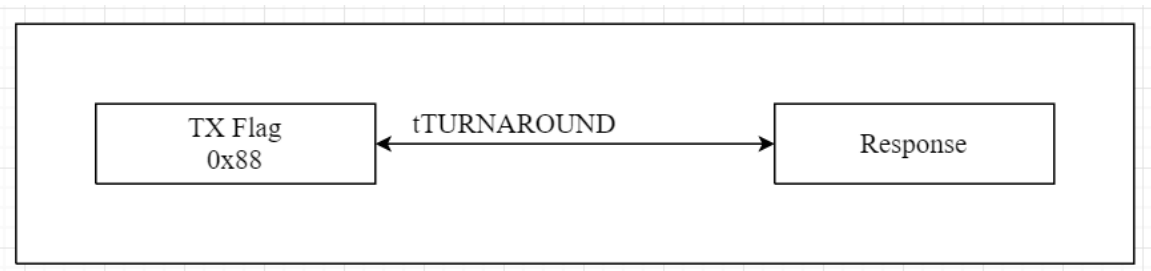


图 3-6 SWI 周转时间时序图

参数	符号	方向 ¹	最小	标准	最大	单位
Start Token	tSTART	输入	4.10	4.34	4.56	μs
		输出	3.91	4.34	4.77	μs
Data Token High	tHIGH	输入	4.10	4.34	4.56	μs
		输出	3.91	4.34	4.77	μs
Data Token Low	tLOW	输入	4.10	4.34	4.56	μs
		输出	3.91	4.34	4.77	μs
Bit Time ²	tBIT	输入	41	43.4	46	μs
		输出	39	43.4	48	μs
Turn Around ³	tTURNAROUND	输入	10			μs
		输出	86	96	106	μs
Bus Timeout ⁴	tTIMEOUT	输入	65			ms

注 1：方向是相对于 SQ713x 设备而言的。输入从主控到 SQ713x，输出从 SQ713x 到主控。

注 2：位计时(Bit Time)：tSTART、tLOW、tHIGH 和 tBIT 设计为与 230.4 kbps 的标准 UART 波特率兼容。UART 设置为 1 个起始位、8 个数据位、无奇偶校验和 1 个停止位。

注 3：周转时间：SQ713x 将在此时间间隔之后启动第一个输出低电平转换，该时间间隔遵循发送标志最后一位的启动脉冲的初始下降沿。在 SQ713x 传输组的最后一个位后，系统必须等待此间隔，然后再发送标志的第一个位。它是从 SQ713x 传输的最后一个比特的启动脉冲的下降沿测量的。

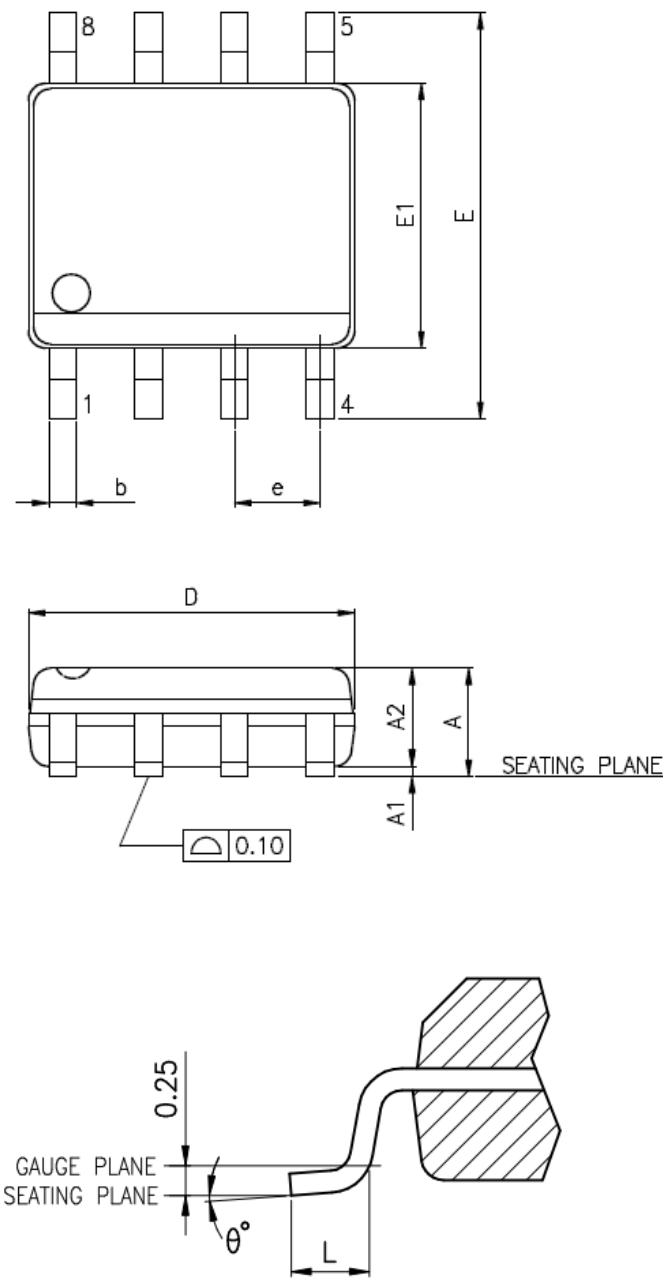
注 4：总线超时：如果总线处于非活动状态的时间超过此持续时间，SQ713x 设备将等待唤醒令牌。

3.7 EEPROM 特性

参数	最小	标准	最大	单位
保证烧写次数 Write Endurance (Sector Endurance)	100,000	-	-	次
数据保留 Data Retention(at 25°C)	100	-	-	年
数据保留 Data Retention(at 85°C)	20	-	-	年

附录 A. 封装信息

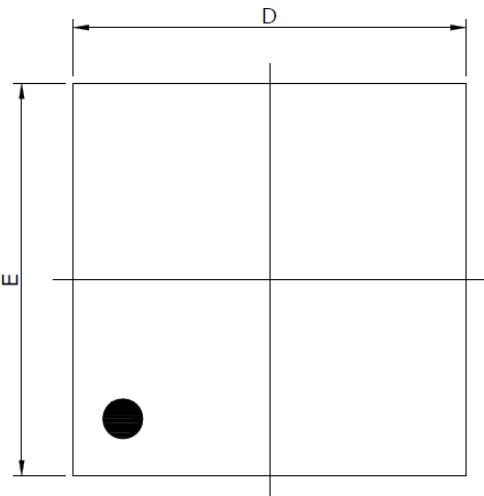
SOP8



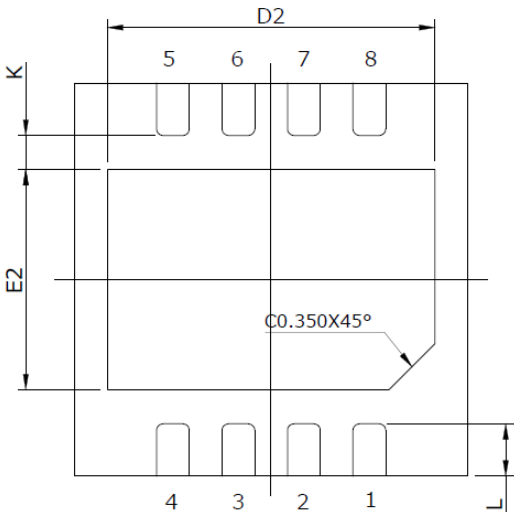
标号	毫米		
	最小值		最大值
A	–	–	1.75
A1	0.10	–	0.25
A2	1.25	–	–
b	0.31	–	0.51
c	0.10	–	0.25
D	4.90 BSC		
E	6.00 BSC		
E1	3.90 BSC		
e	1.27 BSC		
L	0.40	–	1.27
h	0.25	–	0.50
θ	0°	–	8°

No. : TDDS01-S7131-CN (B)	Name : SQ7131/SQ7133/SQ7135 简要中文产品规格书	Version : V 1.7
---------------------------	---------------------------------------	-----------------

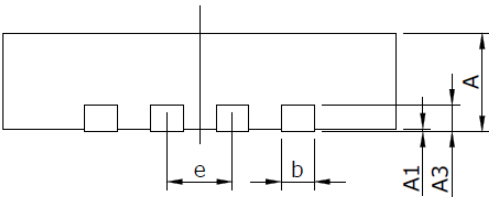
8-Lead DFN (3mm x3mm)



TOP VIEW



BOTTOM VIEW



标号	毫米		
	最小值		最大值
A	0.70	0.75	0.80
A1	0.00	0.02	0.05
A3	0.203 REF.		
b	0.20	0.25	0.30
D	2.90	3.00	3.10
E	2.90	3.00	3.10
e	0.50 BSC		
L	0.35	0.40	0.45
D2	2.35	2.40	2.45
E2	1.65	1.7	1.75
K	0.20	—	—

附录 B. 订购信息

订购产品时，请提供以下详细信息：

订购信息	产品型号	包装	代客烧录	说明
范例	SQ7131SP008C00R	T	Y	I2C, SOP8, Tape & Reel, 85℃, 代客烧录
	SQ7131N3008C00R	B	N	I2C, DFN 3x3, Tray, 85℃, 无代客烧录
	SQ7133SP008S00R	B	Y	SPI, SOP8, Tube, 85℃, 代客烧录
	SQ7133N3008S00R	T	N	SPI, DFN 3x3, Tape & Reel, 85℃, 无代客烧录
	SQ7135SP008W00R	B	Y	SWI, SOP8, Tube, 85℃, 代客烧录
	SQ7135N3008W00R	T	N	SWI, DFN 3x3, Tape & Reel, 85℃, 无代客烧录

注 1: “包装”- T: Tape & Reel; B: Tube/Tray
注 2: “代客烧录”- Y: 需代客烧录; N: 无代客烧录
注 3: 包装- T, SOP: 4K/Reel, DFN: 5K/Reel

附录 C. 产品型号信息

范例：SQ 71 31 SP 008 C 00 R I Y

[illegible][illegible][illegible][illegible][illegible]

代码	封装
SP	SOP
N3	DFN 3x3

[illegible]

代码	脚位数
008	8

[illegible]

代码	类型
C	I2C
S	SPI
W	SWI

内部标识码			
-------	--	--	--

工作温度	
------	--

代码	工作温度
R	-40~85℃

包装	
----	--

代码	包装
T	T&R
B	Tube

烧录服务 _____

代码	烧录
Y	Yes
N	No

修改纪录

版本	发布日期	改版叙述
V1.7	2025/8/5	1. 与 datasheet V1.7 完整版同步
V1.6	2025/4/23	2. 3.6.3 SPI 特性章节增加 SPI 频率 <=55℃ 3. 3.6.3 SPI 特性章节增加 SPI 频率 (VDD=2.0V~2.7V, >55℃), 最大 8 MHz 4. 3.6.3 SPI 特性章节修改 tSO_VD 25 ns 为 40 ns 5. 3.6.3 SPI 特性章节增加注 1 6. 增订附录 B.订购信息 7. 删除附录 D. 使用注意事项 8. 3.3 DC 特性增订工作模式下的供电电流 (非 ECC 命令执行期间) 9. 3.3 DC 特性增订工作模式下的供电电流 (执行 ECC 命令期间)
V1.5	2024/4/18	1. 增订 SQ7135 SWI 相关信息
V1.4	2024/3/5	1. 3.6.3 SPI 特性章节 SPI 时序图新增“ tSPI” 2. 增订附录 B. 产品型号信息
V1.3	2023/12/28	1. 与 datasheet V1.3 完整版同步 2. 增订产品型号 : SQ7131SP008C00R, SQ7131N3008C00R, SQ7133SP008S00R, SQ7133N3008S00R 3. 修订 ECC 指令时的操作电流为 7mA
V1.0	2023/1/18	首次发行