



SQ7131/SQ7133

简要中文产品规格书 V1.0

No. : TDDS01-S7131-CN	Name : SQ7131/SQ7133 简要中文产品规格书	Version : V1.0
-----------------------	--------------------------------	----------------

SQ7131/SQ7133, 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°C ~ 85°C

◆ Communication

- SQ7131 支持 I2C 界面 (Max: 1MHz)
- SQ7133 支持 SPI 界面 (Max: 10MHz)

◆ 安全特性

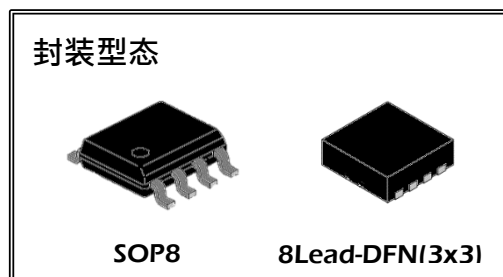
- NIST标准兼容之非对称式硬件加速器, 用于数字签名生成、验证、密钥合意协定
 - NIST P256 / P384 椭圆曲线
 - ECDSA: FIPS 186-4 椭圆曲线数字签名
 - ECDH: FIPS SP800-56A 密钥合意协议(Key Agreement)
- NIST标准兼容硬件对称式加密算法
 - FIPS 180-4 SHA-256 & FIPS 198-1 HMAC 哈希算法
 - FIPS-197 AES-128/256: 加密/解密, Galois Field Multiply for GCM
- 支持网络密钥管理
 - TLS 1.2 & 1.3 PRF/HKDF 计算
 - ECDHE 密钥交换协定(密钥生成、密钥合意协议)
- 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 |



No. : TDDS01-S7131-CN (B)	Name : SQ7131/SQ7133 简要中文产品规格书	Version : V 1.0
---------------------------	--------------------------------	-----------------

Content

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
3. 电气特性.....	7
3.1 极限参数.....	7
3.2 工作条件.....	8
3.2.1 工作条件.....	8
3.2.2 I/O 特性.....	8
3.3 DC 特性.....	9
3.4 上电复位电气特性.....	10
3.5 BROR 电气特性.....	11
3.6 AC 特性.....	12
3.6.1 运行模式时序特性.....	13
3.6.2 I2C 特性.....	13
3.6.3 SPI 特性.....	15
3.7 EEPROM 特性.....	18
附录 A. 封装信息.....	19
附录 B. 使用注意事项.....	21
修改纪录.....	22

No. : TDDS01-S7131-CN (B)	Name : SQ7131/SQ7133 简要中文产品规格书	Version : V 1.0
---------------------------	--------------------------------	-----------------

1. 产品简介

SQ7131/SQ7133 为低功耗安全加密芯片，具备高质量 TRNG 兼容 SP800-22 标准设计要求，支持 NIST 标准兼容之非对称式硬件加速器 ECC384/ECC-256，硬件对称式加密算法 AES-128/AES-256 与 SHA-256。可支持 IoT 设备适用之对称式/非对称式认证，与 TLS1.2/ 1.3 安全通信。高安全性的存储空间，可存储密钥、X.509 压缩证书与数据，存储器槽(slots)详细请参考下表：

Features	SQ7131/SQ7133	Note
Slot	52	
ECC Private Key – 256	7	Slot 1~7
ECC Public Key – 256	4	Slot 24,26,27,28
ECC Private Key – 384	2	Slot 20,21
ECC Public Key – 384	4	Slot 30,32,33,34
ECC Compressed Certificate	2	
AES Key (AES-128/256)	12	Slot 8~19
I/O Protection Key	1	Slot 22
Data	32x6	Slot 36~41
Data	512 x11	Slot 42~52

表 1-1 存储器槽概要

2. 引脚配置

2.1 SQ7131 引脚配置/说明

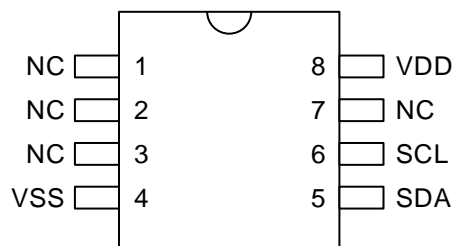


图 2-1 SQ7131 SOP8 封装型态引脚配置

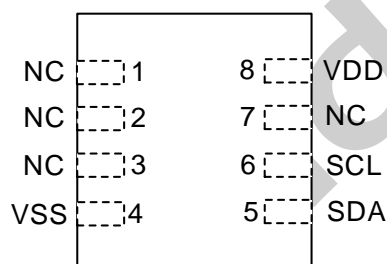


图 2-2 SQ7131 8-Lead DFN 封装型态引脚配置

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

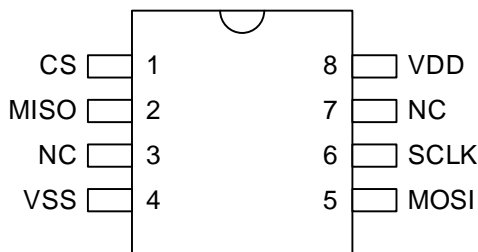


图 2-3 SQ7133 SOP8 封装型态引脚配置

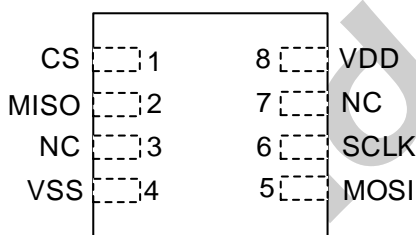


图 2-4 SQ7133 SO7133 8-Lead DFN 封装型态引脚配置

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

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
工作电压范围	V_{DD}		-0.3 to 6.0	V
输入电压范围	V_{IN}	All I/O pins	-0.3 to $V_{DD}+0.3V$	V
最大输出电流(总和)	I_{OL}	All I/O pins	50	mA
保存温度范围	T_{STG}		-50 to 125	°C

No. : TDDS01-S7131-CN (B)	Name : SQ7131/SQ7133 简要中文产品规格书	Version : V 1.0
---------------------------	--------------------------------	-----------------

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°C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	°C

3.2.2 I/O 特性

参数	符号	最小	标准	最大	单位
低电压输入	V _{IL}	0		0.3 VDD	V
高电压输入	V _{IH}	0.7 VDD		VDD	V
端口引脚之低电压输出	V _{OL}	0		0.1VDD	V
端口引脚之高电压输出	V _{OH}	0.9VDD		VDD	V

No. : TDDS01-S7131-CN (B)	Name : SQ7131/SQ7133 简要中文产品规格书	Version : V 1.0
---------------------------	--------------------------------	-----------------

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)	I_{DD_N1}		3.7		mA
深眠模式(Deep Sleep Mode)下的操作电流	I_{DD_DS}		0.8		uA

Note :此状态为等待 Command 期间，执行指令期间的操作电流，请参考附录 B。

No. : TDDS01-S7131-CN (B)	Name : SQ7131/SQ7133 简要中文产品规格书	Version : V 1.0
---------------------------	--------------------------------	-----------------

3.4 上电复位电气特性

Ta=-40~85°C					
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 CPU ready 时间 Warming-up time after a reset is clear and CPU ready	-	4	-	ms
tVDD	上电时间 Power supply rise time	0.5		5	ms

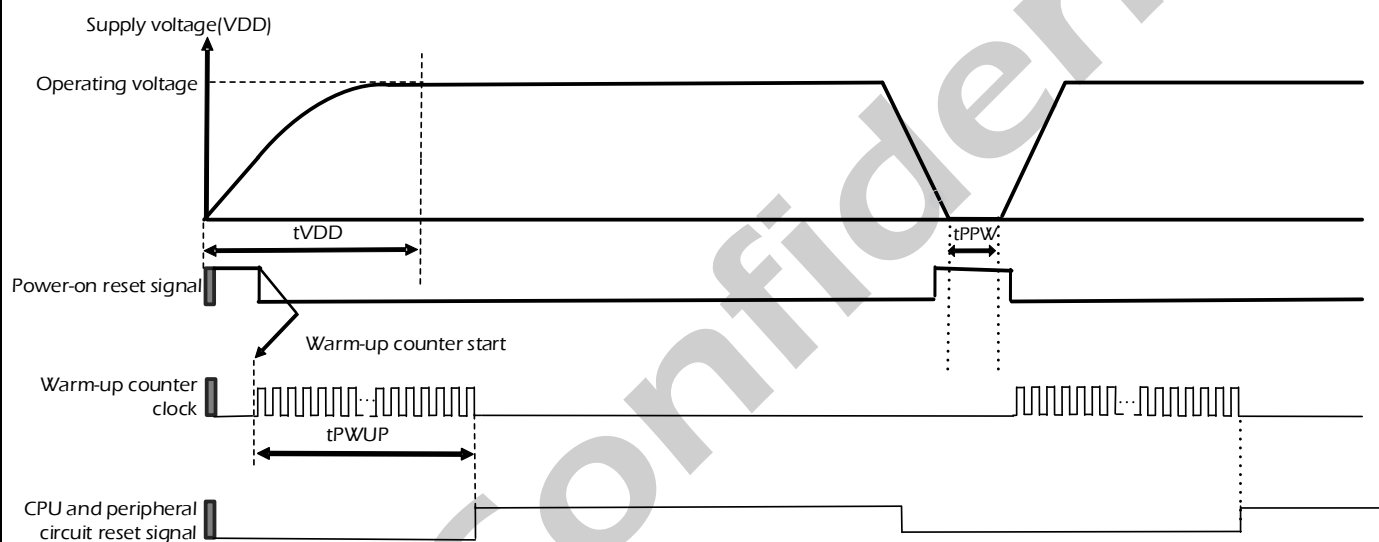


图 3-1 上电复位时序图

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。

No. : TDDS01-S7131-CN (B)	Name : SQ7131/SQ7133 简要中文产品规格书	Version : V 1.0
---------------------------	--------------------------------	-----------------

3.5 BROR 电气特性

Ta=-40~85°C						
参数	符号	测试条件	最小	标准	最大	单位
BROR 检测电压	VBROR_Rising	VDD rise time and fall time > tVDD (tVDD please refer to Ch3.4 Power-on Reset Characteristics)	1.95	2.0	2.05	V
	VBROR_Falling		1.85	1.90	1.95	V

No. : TDDS01-S7131-CN (B)	Name : SQ7131/SQ7133 简要中文产品规格书	Version : V 1.0
---------------------------	--------------------------------	-----------------

3.6 AC 特性

参数	符号	测试条件	最小	标准	最大	单位
上电延时 (Note3) Power-Up Delay	T_{PU}	从 $VSS > VSS_{min}$ 到 t_{WLO} 开始的最短时间	100	-	-	us
唤醒为低电平的持续时间 Wake Low Duration	T_{WLO}		60	-	-	us
唤醒为高电平到数据通信的延时 Wake High Delay to Data Comm	T_{WHI}	除非实现了轮询，否则SDA 在整个过程中应保持稳定的高电平状态。上电时不启动SelfTest。	1500	-	-	us
启动 SelfTest 时的唤醒为高电平延时 Wake High Delay when SelfTest is Enabled	T_{WHIST}	除非实现了轮询，否则SDA 在整个过程中应保持稳定的高电平状态。	20	-	-	ms
看门狗超时 Watchdog Timeout	T_{WATC} $HDOG$	从唤醒到强制 IC 进入休眠模式的时间 Config.ChipMode[2]为 0.	0.7	1.3	1.7	us

Note 1 : Writer cycle time 包含数据更新

Note 2 : 这些参数为特性值，但未经生产测试。

Note 3 : 方向-“至加密器件(To crypto Authentication)”

Note 4 : 如果在配置区中启动了上电自检，则上电延时将显著延长

No. : TDDS01-S7131-CN (B)	Name : SQ7131/SQ7133 简要中文产品规格书	Version : V 1.0
---------------------------	--------------------------------	-----------------

3.6.1 运行模式时序特性

参数	符号	最小	标准	最大	单位
上电就绪时间 Power-Up Ready Time	T_{PU_RDY}		1200	1500	μS
Standby 时间 · 进入 deep sleep 模式 Standby Time, Entering the deep sleep mode	T_{STB}		55	90	μS
唤醒就绪时间 · deep sleep 模式 Wake-Up Ready Time, deep sleep mode	T_{WDS_RDY}		300	-	μS

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}	0	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	-	μs
SCL 时钟低电平周期 (Low Period of SCL Clock)	t_{LOW}	0.65	-	μs
SCL 时钟高电平周期 (High Period of SCL Clock)	t_{HIGH}	0.35	-	μs
重启条件设置时间 (Setup Time for a Repeated START Condition)	$t_{SU;STA}$	0.35	-	μs
数据保持时间 (Data Hold Time)	$t_{HD;DAT}$	-	0.5	μs
数据设置时间 (Data Setup Time)	$t_{SU;DAT}$	0.1	-	μs
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	-	μs
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	-	μs
每条总线之电容负载 (Capacitive Load for each Bus Line)	C_b	-	400	pF

No. : TDDS01-S7131-CN (B)	Name : SQ7131/SQ7133 简要中文产品规格书	Version : V 1.0
---------------------------	--------------------------------	-----------------

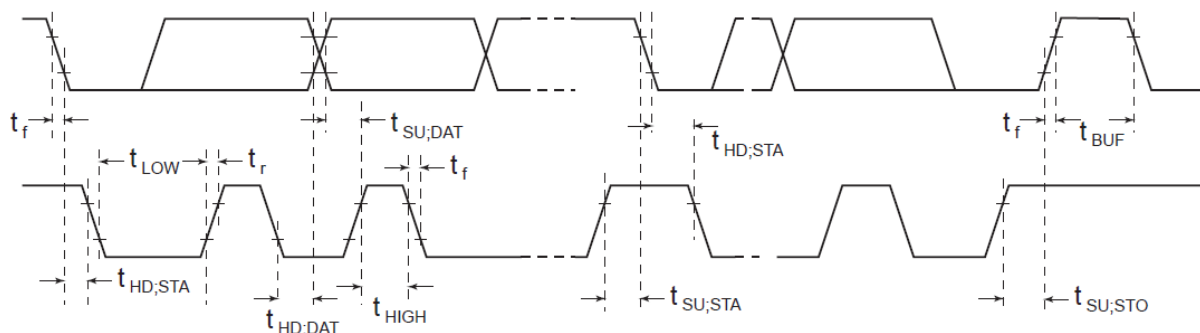


图 3-2 I2C 时序图

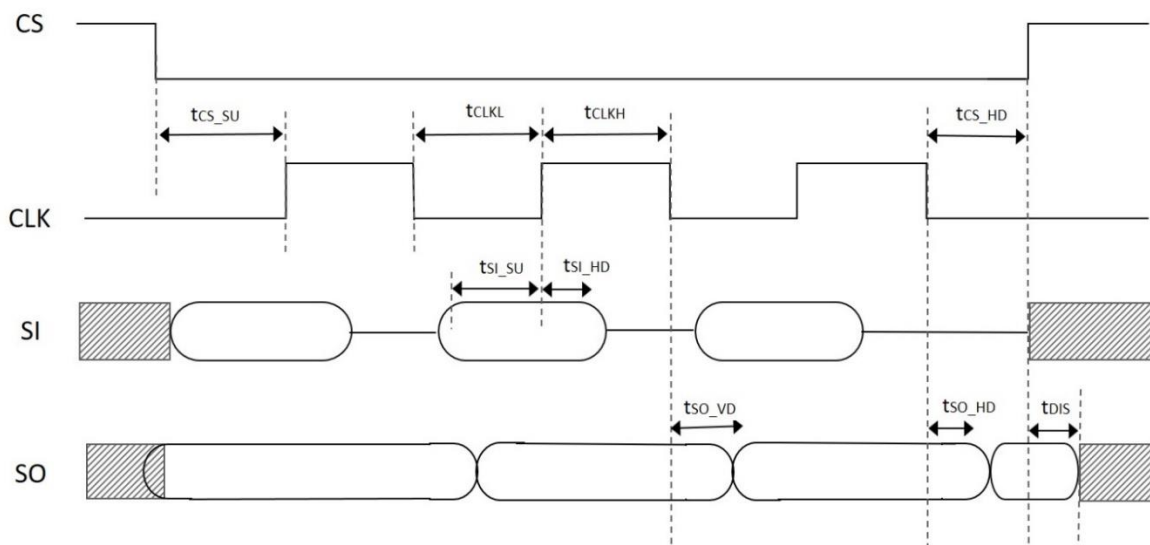
No. : TDDS01-S7131-CN (B)	Name : SQ7131/SQ7133 简要中文产品规格书	Version : V 1.0
---------------------------	--------------------------------	-----------------

3.6.3 SPI 特性

(VDD=2.7V~5.5V)				
参数	符号	最小	最大	单位
SPI 频率 SPI Frequency	f_{SPI}		10	MHz
SPI 周期 SPI Period	t_{SPI}	100		ns
SCLK 高电平周期 High period of the SCLK pin	t_{CLKH}	40		ns
SCLK 低电平周期 Low period of the SCLK pin	t_{CLKL}	40		ns
从 SPICS 有效到第一个边沿的时间 From SPICS active to first edge	t_{CS_SU}	20		ns
从最后一个 SCLK 边沿到 SPICS 无效的时间 From last SCLK edge to SPICS inactive	t_{CS_HD}	20		ns
SPI 传输时间 Time between SPI transaction	t_{CS_WA}	(1)		us
输入数据设置时间 Data Input Setup Time	t_{SI_SU}	5		ns
输出数据保持时间 Data Input Hold time	t_{SI_HD}	5		ns
输出数据有效时间 Data Output Valid Time	t_{SO_VD}		20	ns
输出数据保持时间 Data Output Hold Time	t_{SO_HD}	0		ns
输出数据禁止时间 Data Output Disable Time	t_{SO_DIS}		20	ns

No. : TDDS01-S7131-CN (B)	Name : SQ7131/SQ7133 简要中文产品规格书	Version : V 1.0
---------------------------	--------------------------------	-----------------

(VDD=2.0V~2.7V)				
参数	符号	最小	最大	单位
SPI 频率 SPI Frequency	f_{SPI}		5	MHz
SPI 周期 SPI Period	t_{SPI}	200		ns
SCLK 高电平周期 High period of the SCLK pin	t_{CLKH}	80		ns
SCLK 低电平周期 Low period of the SCLK pin	t_{CLKL}	80		ns
从 SPICS 有效到第一个边沿的时间 From SPICS active to first edge	t_{CS_SU}	40		ns
从最后一个 SCLK 边沿到 SPICS 无效的时间 From last SCLK edge to SPICS inactive	t_{CS_HD}	40		ns
SPI 传输时间 Time between SPI transaction	t_{CS_WA}	(2)		us
输入数据设置时间 Data Input Setup Time	t_{SI_SU}	10		ns
输出数据保持时间 Data Input Hold time	t_{SI_HD}	10		ns
输出数据有效时间 Data Output Valid Time	t_{SO_VD}		40	ns
输出数据保持时间 Data Output Hold Time	t_{SO_HD}	0		ns
输出数据禁止时间 Data Output Disable Time	t_{SO_DIS}		40	ns



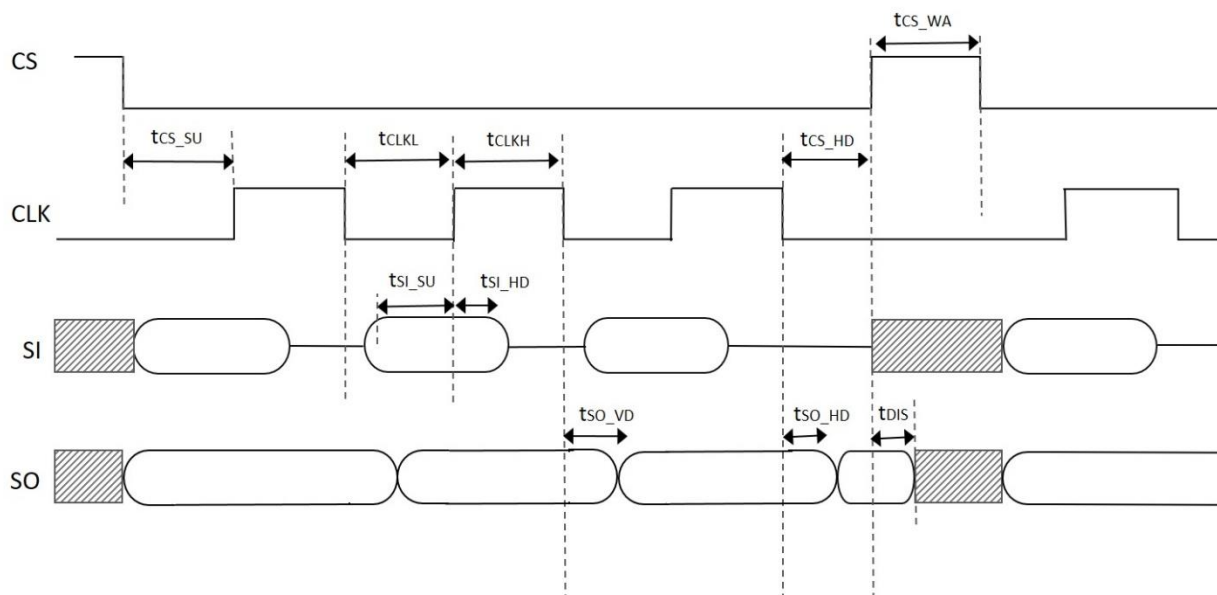


图 3-3 SPI 时序图

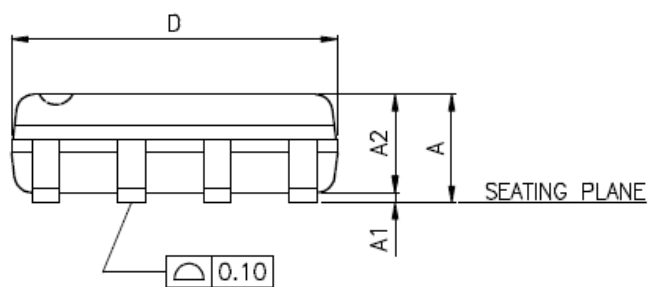
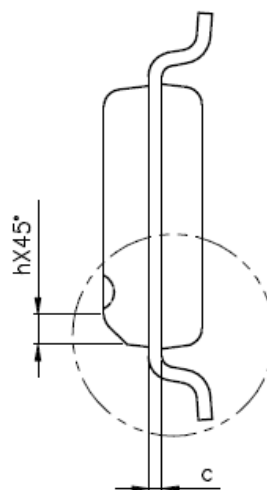
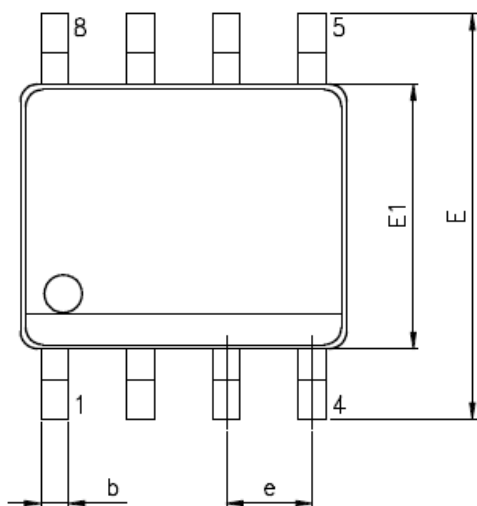
3.7 EEPROM 特性

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

No. : TDDS01-S7131-CN (B)	Name : SQ7131/SQ7133 简要中文产品规格书	Version : V 1.0
---------------------------	--------------------------------	-----------------

附录 A. 封装信息

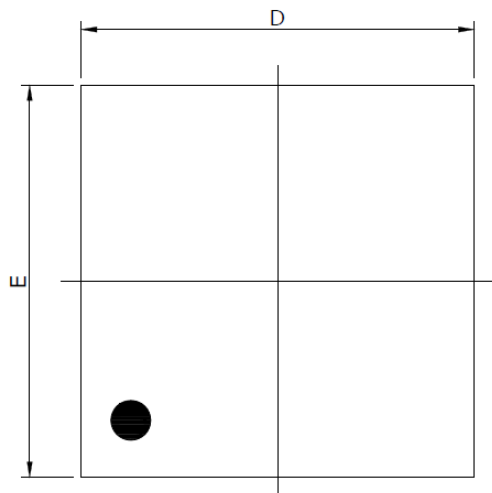
SOP8



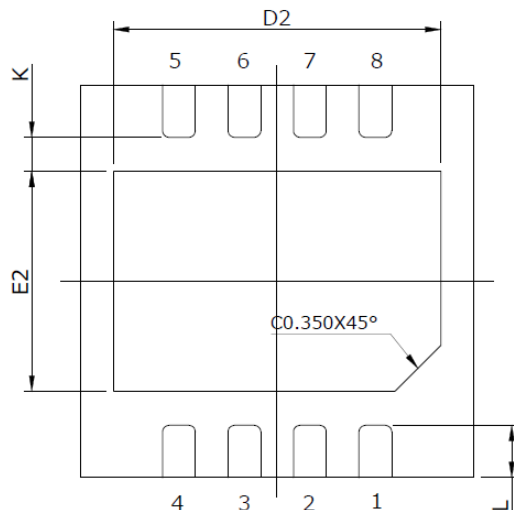
标号	毫米		
	最小值		最大值
A	-	-	1.75
A1	0.10	-	0.25
A2	1.25	-	-
b	0.31	-	0.51
c	0.10	-	0.25
D	4.90 BSC		
E	6.00 BSC		
E1	3.90 BSC		
e	1.27 BSC		
L	0.40	-	1.27
L1	1.00 REF		
h	0.25	-	0.50
θ	0°	-	8°

No. : TDDS01-S7131-CN (B)	Name : SQ7131/SQ7133 简要中文产品规格书	Version : V 1.0
---------------------------	--------------------------------	-----------------

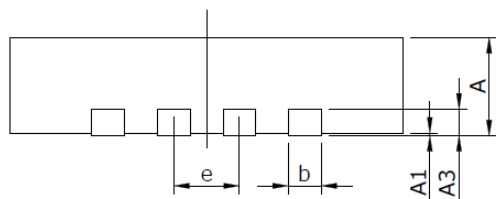
8-Lead DFN (3x3)



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	2.45	2.50	2.55
E2	1.63	1.68	1.73
K	0.20	-	-

No. : TDDS01-S7131-CN (B)	Name : SQ7131/SQ7133 简要中文产品规格书	Version : V 1.0
---------------------------	--------------------------------	-----------------

附录 B. 使用注意事项

(A) DC 特性相关:

运行模式(Operation Mode)下的操作电流参考值，请参考下表：

参数	符号	最小	标准	最大	单位
等待指令时的操作电流	I_{DD_N1}		3.7		mA
执行 non-ECC 指令时的操作电流	I_{DD_N2}		4.3		mA
执行 ECC 指令时的操作电流	I_{DD_N3}		9.2		mA

No. : TDDS01-S7131-CN (B)	Name : SQ7131/SQ7133 简要中文产品规格书	Version : V 1.0
---------------------------	--------------------------------	-----------------

修改纪录

版本	发布日期	改版叙述
V1.0	2023/1/18	首次发行