BT1005 Security IC with 1Kb I²C EEPROM

简介和特性

BT1005 为用户有效地提供加密和认证的解决方案，可以广泛用于系统的知识产权保护，防 PCB 抄板，防止 IC 集成电路的反向和克隆，以及系统软件保护。BT1005 使用工业界标准的 I^2C 接口与主机进行认证通讯，系统实现简单。认证采用国际认可的高强度算法，用户密钥 128 位，被公认无法破解。

BT1005 为用户提供 1K 位的 EERPOM 空间，用户可以自由存储数据。EEPROM 的读写次数保证在 20 万次以上(25°C)。

BT1005 采用 CMOS 工艺，功耗极省。在无认证操作的等待状态下，其功耗<1uW，非常适合应用在手机，手提电脑，掌上游戏机等使用电池的系统平台上。

功能特点

- 采用高强度算法和专用硬件加/解密引擎
- 1024 位 EEPROM 用户存储空间
- 支持待机节电模式。在节电模式下，功耗极省 (节电模式功耗<1uW)
- 128 位密钥，一次性烧录，不可读。64 位明文及密文寄存器
- 支持 24 位客户 ID 功能，有效加强用户密钥的安全性
- 支持 400Kpbs 的 I^2C 的通讯速率，支持多字节读写方式
- 内置时钟电路和复位电路，所需外围元件极少
- 宽电压输入，3.0V – 5.5V，适用范围广
- 工作温度范围： -40 - 85°C
- 8-pin SOP，TSSOP 和 MSOP 封装选择

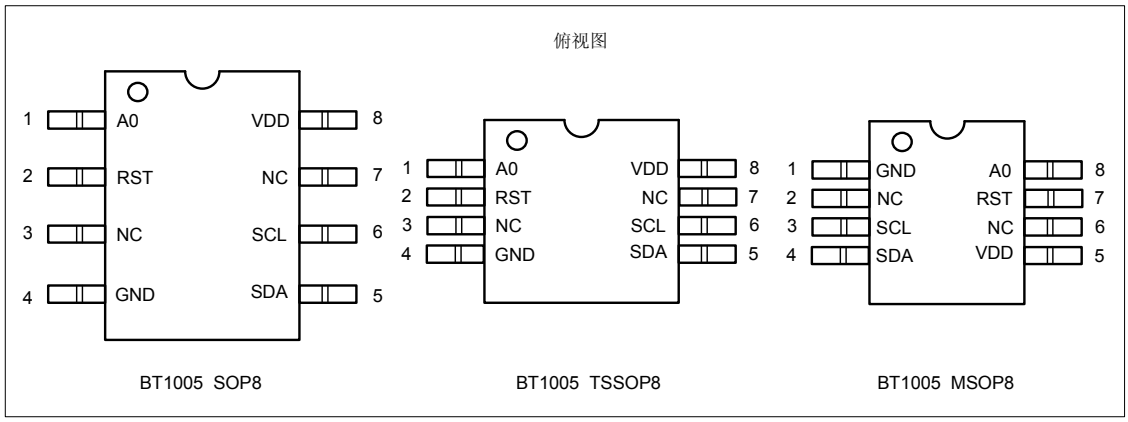
订购规格

型号	封装	温度范围
BT1005-E	SOP8	-40-85°C
BT1005-S	TSSOP8	-40-85°C
BT1005-T	MSOP8	-40-85°C

应用范围

手机，DVD，数字电视，数字机顶盒，导航仪，平板电脑，游戏机，电子阅读器，数码相机/摄像机，MP3/MP4 Audio/Video 播放器，FPGA IP 保护 ，授权证书管理...

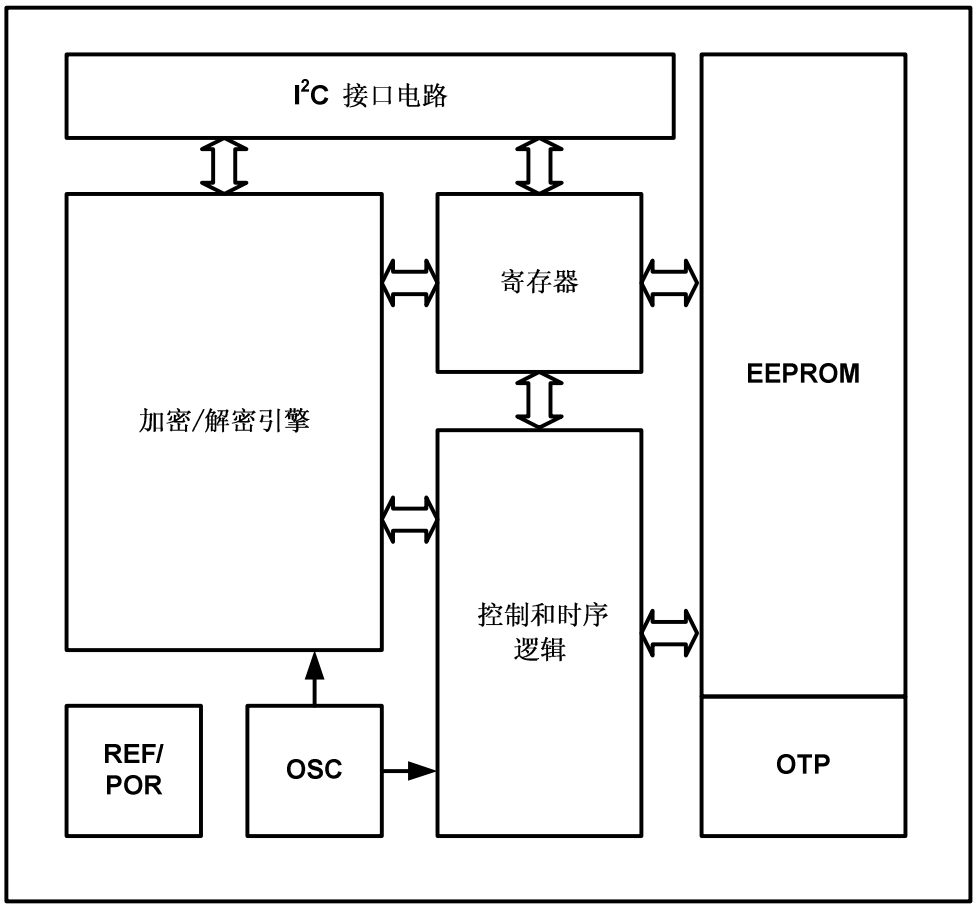
管脚排列



管脚定义

封装类型			管脚名称	端口方向	功能描述
SOP8	TSSOP8	MSOP8			
1	1	8	A0	输入	I^2C 地址选择
2	2	7	RST	输入	初始化(Reset), 高电平有效
3	3	2	NC	n/a	保留 Reserved，正常使用时接地
4	4	1	GND	电源	接地
5	5	4	SDA	输入/输出	I^2C 数据线，使用时需外接上拉电阻
6	6	3	SCL	输入	I^2C 时钟线，使用时需外接上拉电阻
7	7	6	NC	n/a	保留 Reserved，正常使用时悬空
8	8	5	VDD	电源	电源

功能框图



寄存器地址

地址	读写类型	功能描述
0x00-0x7F	读/写	EEPROM 用户区域 (1K bits, or 128x8bit)，读支持 I²C 多字节方式
0x80-0x8F	一次写，不可读	128 位密钥 128-bit key, OTP 区域。
0x90-0x97	读/写	密文寄存器，读写支持 I²C 多字节方式
0x98-0x9F	只读	明文寄存器，读支持 I²C 多字节方式
0xA0-0xA2	只读	客户 ID 寄存器，读支持 I²C 多字节方式
0xF0	读/写	待机节电模式 Power Down， 0x00:工作模式，0x01:节电模式

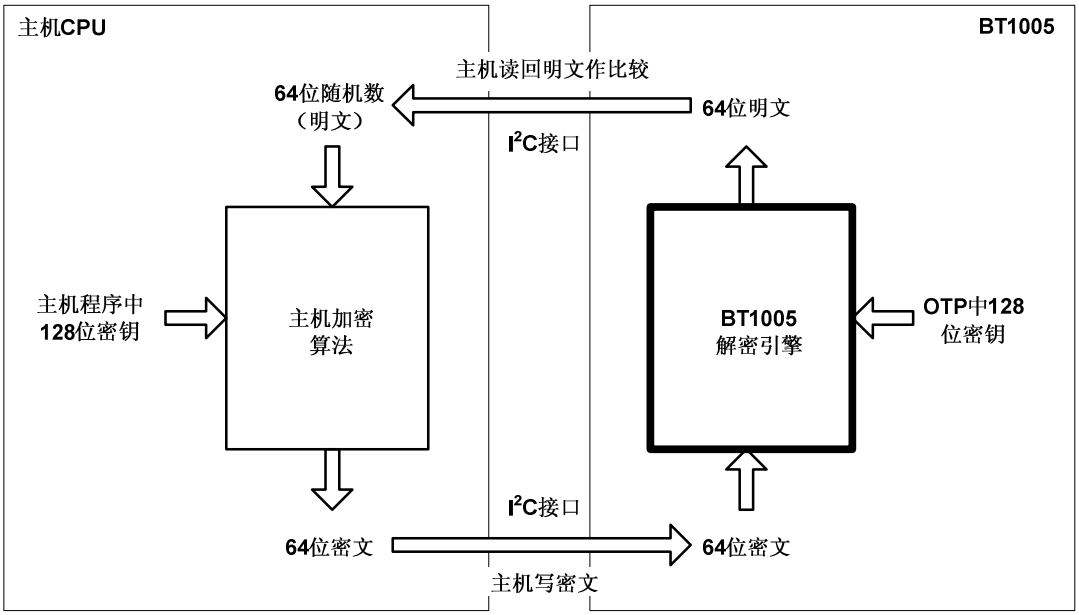
功能介绍

加/解密功能概述

BT1005 的验证过程首先是由主机(CPU)程序产生一个 64 位的随机数(明文)，然后由主机加密程序对此明文进行加密，加密所用的 128 位密钥和 BT1005 的 OTP 中存储的密钥是相同的。加密后得到的 64 位密文通过 I^2C 由主机发送到 BT1005。

BT1005 的密文寄存器(0x90-0x97)由 8 个字节组成，用来接收主机传来的 64 位密文。当主机通过 I^2C 完成对密文寄存器的第 8 个字节(0x97)的写操作后，BT1005 的解密引擎即刻启动，进行解密运算。解密后得到的明文被放置在明文寄存器(0x98-0x9F)，供主机读回。由于 BT1005 采用的是专用硬件计算引擎，解密速度快，主机在写完密文之后，可以立即读取解密后的明文，而无需等待。

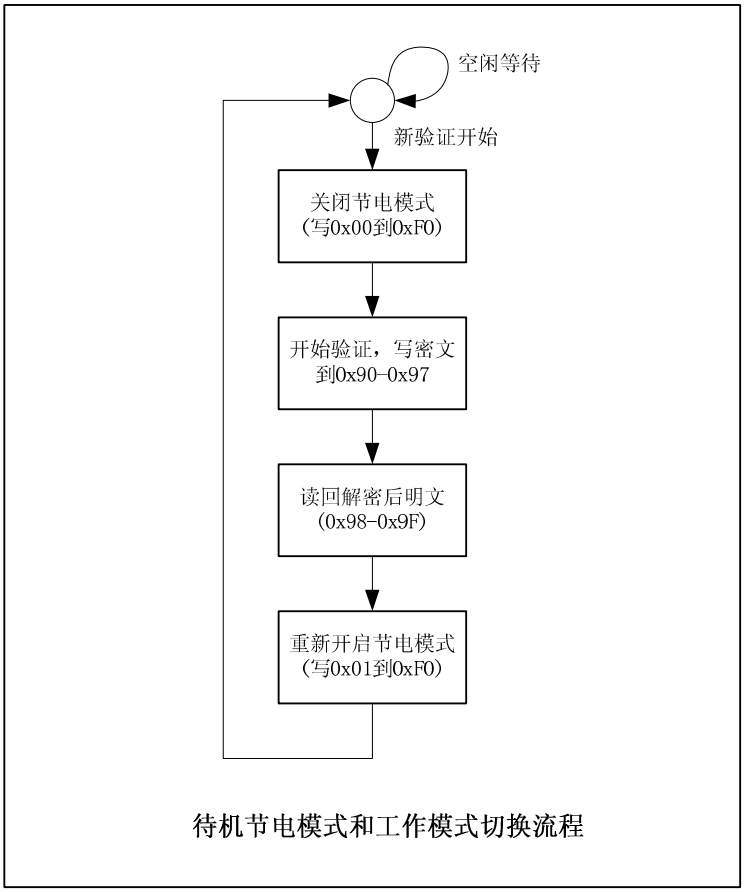
主机通过 I^2C 将明文从 BT1005 的明文寄存器读回后，和原先的明文(64 位随机数)进行比较。如果两者相同，则验证通过。如果两者不同，则验证失败。主机程序依照此验证的结果，进行相应的操作。



注: 主机程序中的密钥和BT1005中OTP的密钥相同；如果主机读回的明文和原来的明文(随机数)相同，则验证成功。

BT1005 设有节电模式。当节电模式寄存器(0xF0)被写入 0x01 时，节电功能开启，这时芯片处于等待状态(Stand-by)，BT1005 的功耗小于 1uW。如要退出节电模式，可以在节电寄存器(0xF0)中写入 0x00， 或者重置(Reset)BT1005。在 BT1005 重新上电(Power-on)或重置(Reset)后，节电模式的缺省状态是被禁止。

当 BT1005 处于节电模式时，如果要进行新的验证过程，必须在主机写密文前关闭节电模式。在主机读回明文结果后，可以再开启节电模式，将芯片设置于待机状态。

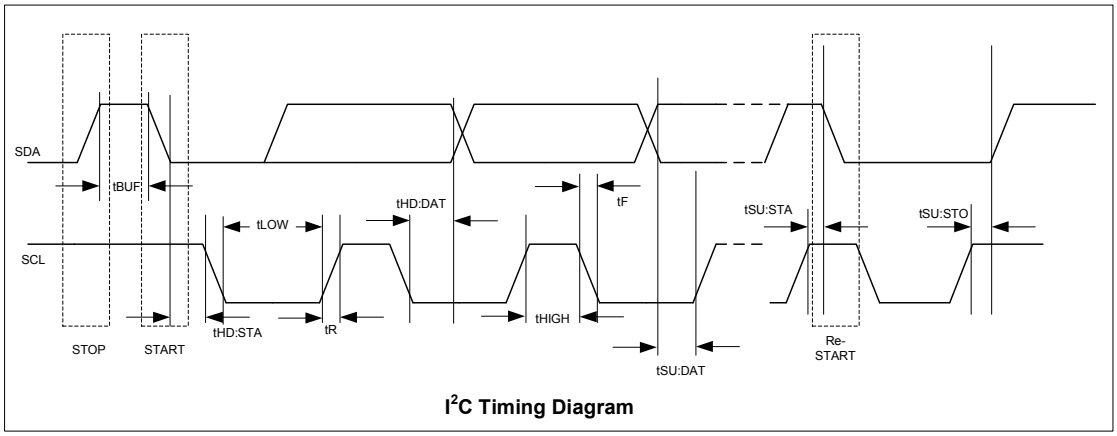


待机节电模式和工作模式切换流程

BT1005 提供 24 位客户 ID 功能。客户 ID 寄存器由 3 个字节组成(0xA0-0xA2)，为只读寄存器。客户 ID 在芯片出厂时一次性烧录，用户不可更改。客户 ID 功能能够有效地提高用户密钥的安全性。同时，通过和认证算法的结合，客户 ID 还可以为用户系统提供 ID，以便系统的激活和授权功能的实现。

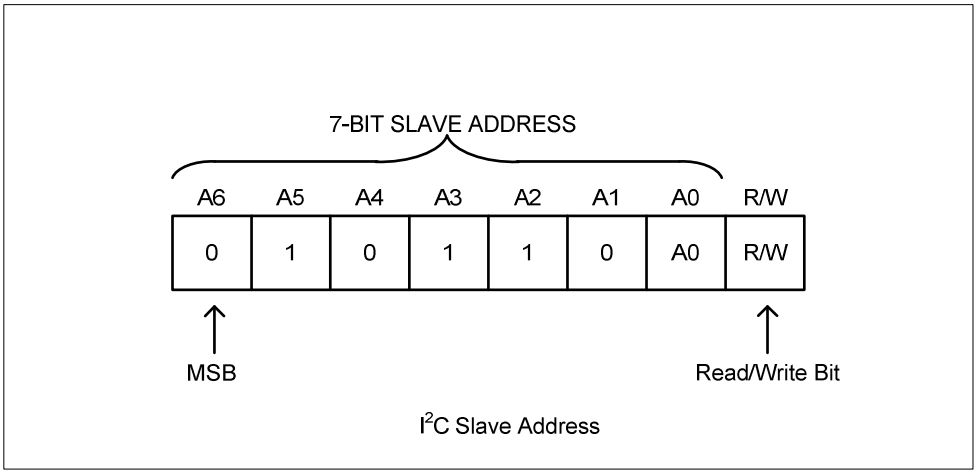
I^2C 接口功能和时序

主机和 BT1005 之间的通讯是通过 I^2C 接口来实现的。BT1005 的 I^2C 接口由一条数据线(SDA)和一条时钟线(SDA)组成。在搭建系统的时候，这两条线都需要上拉电阻。主机(CPU)是 I^2C 的主控方(Master), BT1005 是 I^2C 的受控方(Slave)。数据在 I^2C 总线上的传输是以字节为单位，而每个字节里的 8 位数据，传输的顺序是高位(Most Significant)在前，低位(Least Significant)在后。每个字节传输结束后还有一位响应位(Acknowledge)。I^2C 的时序请参照下图。详细的时间参数请参照附后的 I^2C 时序参数表。



I²C Timing Diagram

BT1005 的 Slave 地址长度为 7 位，是由“010110”和 A0 位组成(如下图所示)。通过选取 A0 的值，BT1005 的 I²C 地址可以设成(2C)Hex 或者(2D)Hex。

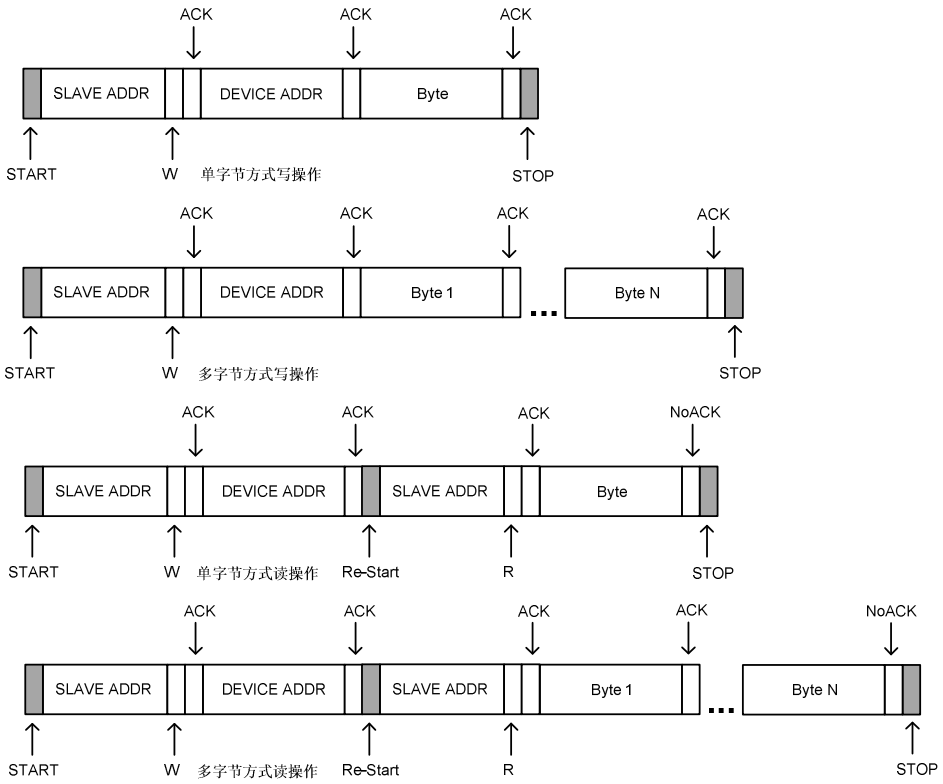


I²C Slave Address

A0 设置	A0 接 GND	A0 接 VDD
I²C Slave Address	0x2C	0x2D

BT1005 的 I²C 接口支持 100kbps 的标准速率(Standard Mode)，或者 400kbps 的快速速率(Fast Mode)。

BT1005 的 I²C 支持单字节读写和多字节读写方式。单字节读写方式每次只能对选定地址的单个字节进行读写，而多字节读写方式每次读写可以完成以选定地址为起始地址的多字节的读写。在多字节方式下，BT1005 的 I²C 控制器在完成每个字节的读写以后，自动累加读写地址。



I²C单/多字节读写数据格式

BT1005 的地址中适用于多字节读的地址范围有 0x00-0x7F，0x90-0x9F 和 0xA0-0xA2，而适用于多字节写的地址范围只有 0x90-0x97(明文寄存器)。对于 0x00-0x7F 的写操作，由于 EEPROM 写时序的要求，BT1005 只支持单字节方式，并且单字节写操作之间应该有不小于 10ms 的间隔。

最大额定参数

SYMBOL	PARAMETER	VALUE	UNIT
Vmax	Voltage on Any Pin Relative to Ground	-0.5-6.0	V
Toper	Operating Temperature	-40-85	℃
Tjmax	Junction Temperature Max	150	℃
Tstorage	Storage Temperature	0-125	℃
Tsold	Soldering Temperature (10 Seconds)	300	℃

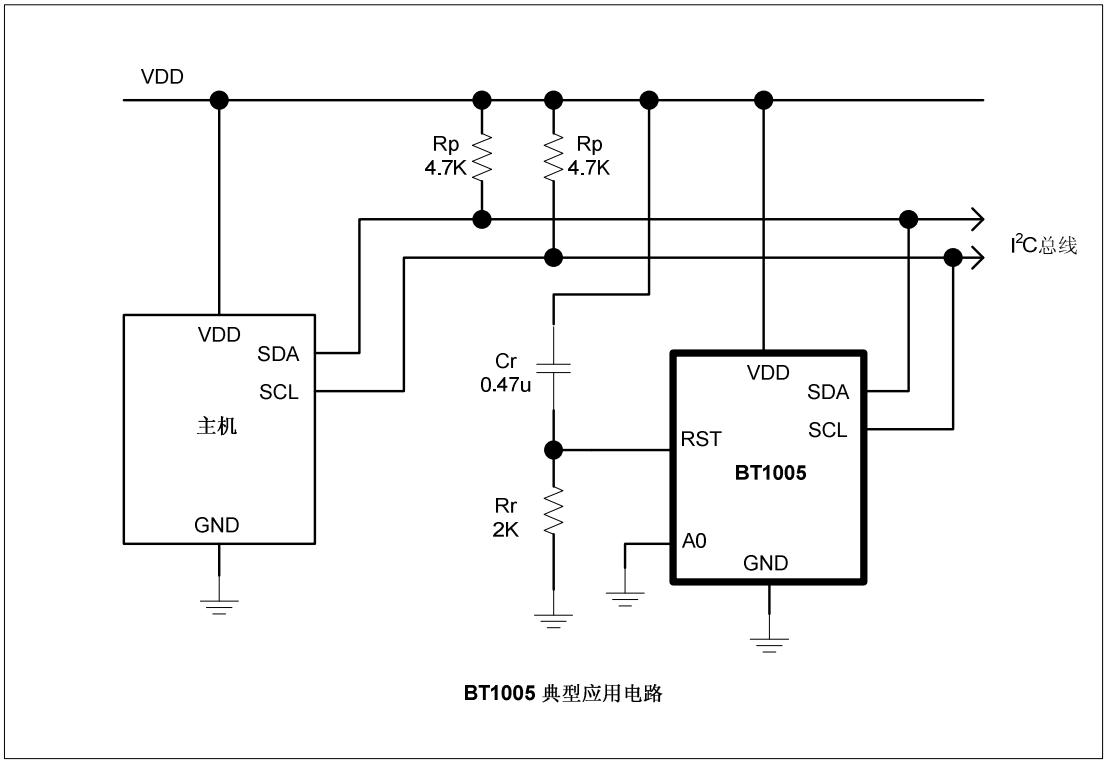
电器特性

SYMBOL	PARAMETER	MIN	TYP	MAX	UNIT
V_{DD}	Power Supply	3.0		5.5	V
V_{IL}	Input Low Voltage			0.8	V
V_{IH}	Input High Voltage	2.0			
V_{OL}	Output Low Voltage			0.4	
V_{OH}	Output High Voltage	2.4			
I_{OZ}	Tristate Output Leakage Current	-10		10	uA
I_L	Input Leakage Current	-10		10	uA
T_J	Junction temperature	0	25	70	℃

I^2C 时序参数表

PARAMETER	SYMBOL	MIN	MAX	UNIT
SCL Clock Frequency	fSCL		400	KHz
Hold-Time (Repeated) Start Condition	tHD:STA	0.6		μs
SCL Clock Low Period	tLOW	1.3		μs
SCL Clock High Period	tHIGH	0.6		μs
Setup-Time for a Repeated Start Condition	tSU:STA	0.6		μs
Data Hold Time	tHD:DAT	0.0	0.9	μs
Data Setup Time	tSU:DAT	100		ns
Rise time for both SDA and SCL signals	tR	20	300	ns
Fall time for both SDA and SCL signals	tF	20	300	ns
Setup Time for a Stop Condition	tSU:STO	0.6		μs
Bus Free Time Between a Stop and Start	tBUF	1.3		μs
Capacitive Load for Each Bus Line	Cb		400	pF

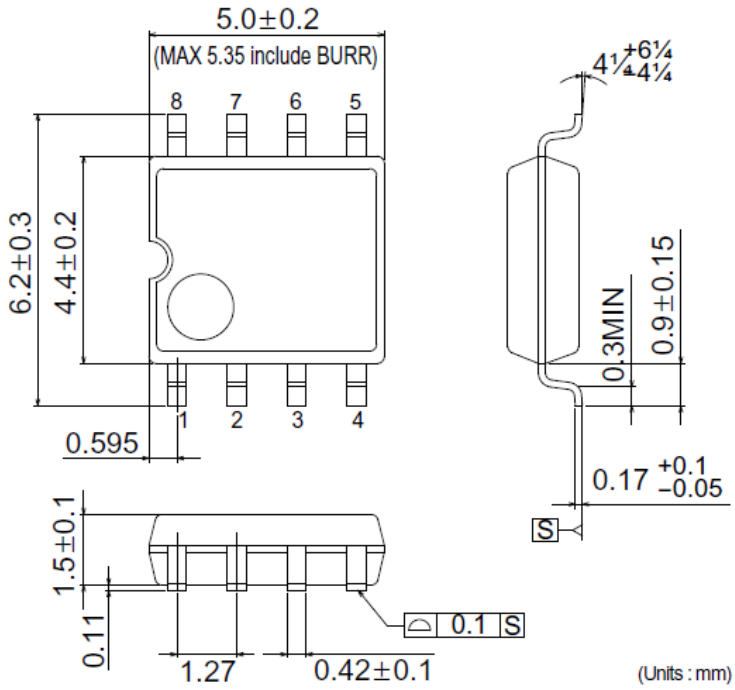
典型应用电路



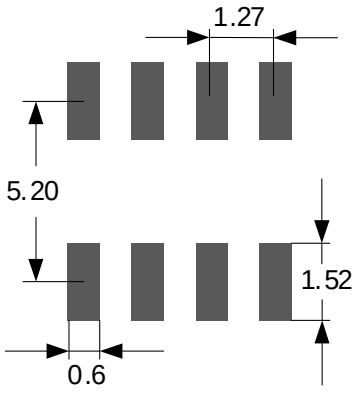
BT1005 典型应用电路

注：Rp 为 SDA 和 SCL 信号线提供上拉电阻。Rr 和 Cr 组成 RC 电路为 BT1005 提供上电时的外部复位。由于 BT1005 设置了内部复位电路，因此 Rr 和 Cr 可以省略，而把 RST 脚直接连到 GND。RST 脚也可以直接连接到主机 CPU 的一个 IO 口，从而让 BT1005 的复位受控于主机。

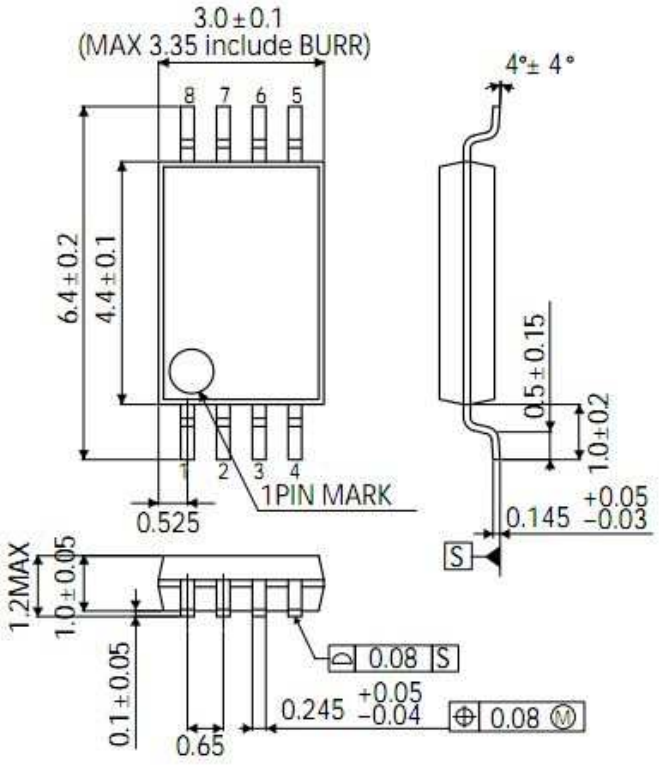
封装 SOP-8 Package



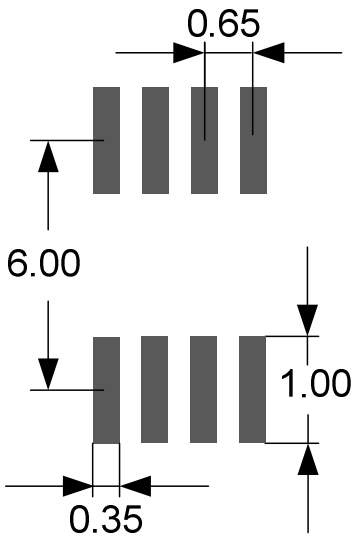
PCB Soldering Footprint (For Reference Only):



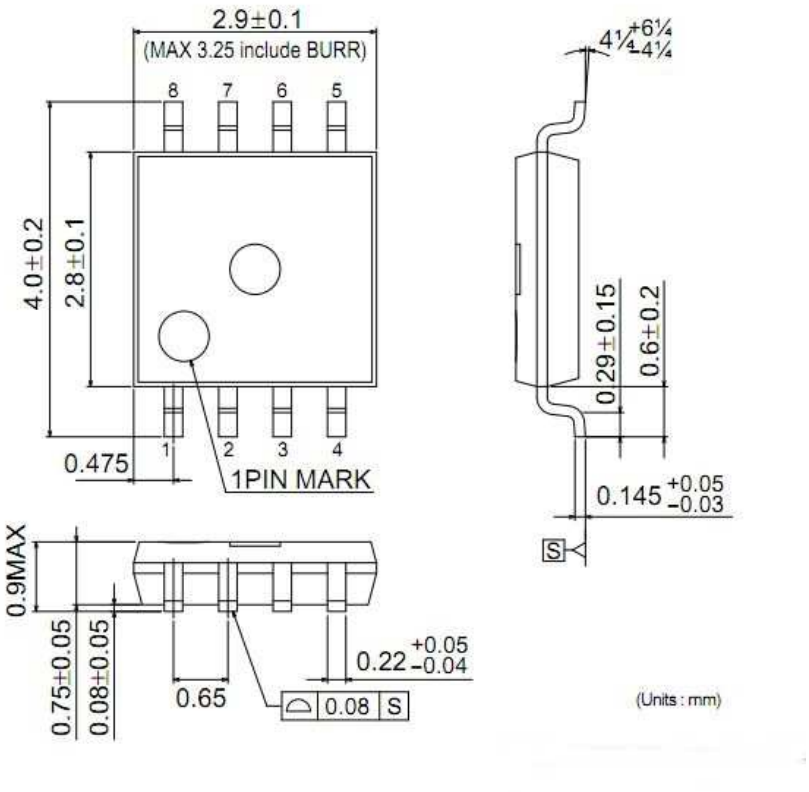
封装 TSSOP8 Package



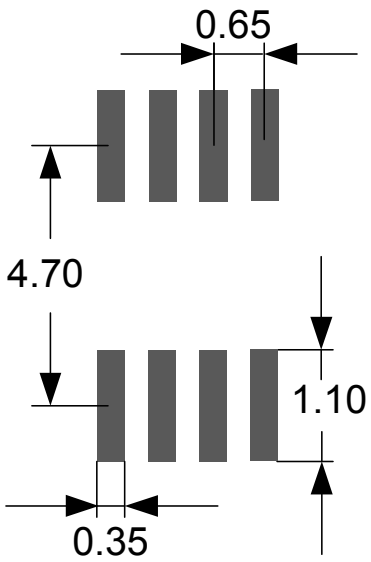
PCB Soldering Footprint (For Reference Only):



封装 MSOP-8 Package



PCB Soldering Footprint (For Reference Only):



Revision History

Revision Number	Revision Date	Description
1.0	Mar 2010	Initial Release
1.1	February 2011	RST changes to active high, and other minor changes
1.2	Sept. 2011	Added 2 more package types