LKT4202U　32 位加密芯片

开发手册

凌科芯安科技（北京）有限公司

第 1 章 LKT4202U 芯片硬件特性

1.1 芯片参数

CPU

- 32位安全CPU内核
- CPU内频最高48MHz

片上存储

- 14KB 文件密钥存储区

Flash 寿命

- 不低于10万次擦写次数或10年有效存储

数据安全机制

- 硬件真随机数发生器
- 唯一ID号
- CRC16 硬件计算模块
- DES/TDES/AES/硬件协处理器
- 有效防止DPA/SPA 攻击机制
- 具有过/欠压传感器
- 内存数据动态加密
- 优化安全布局
- 多达2048位的RSA硬件协处理器

奇偶校验/ CRC计算器

- 8 / 16 / 32位奇偶校验
- CRC-16/32 计算器

IIC通讯接口

- IIC 从模式
- 支持硬件 IIC 总线协议
- 支持通讯速率最高400Kbps

复位

- 上电冷复位
- 热复位

操控特性

- 单电源：1.62V ~ 5.5V
- 工作温度：- 25 ℃ ~+ 85℃
  - 40 ℃ ~+ 85℃（可定制）
- 正常工作电流 6mA
- 低功耗模式电流（关断模式） 0.1uA
- ESD保护大于6000V（HBM）

1.2 引脚定义

引脚序号	引脚名称	功能描述	引脚类型
1	RST	复位	输入
2	NC	---	
3	NC	---	
4	GND	地	输入
5	SDA	IIC_SDA	输入/输出
6	SCL	IIC_SCL	输入
7	NC	---	
8	VCC	电源	输入

表1-1：LKT4202U 引脚说明

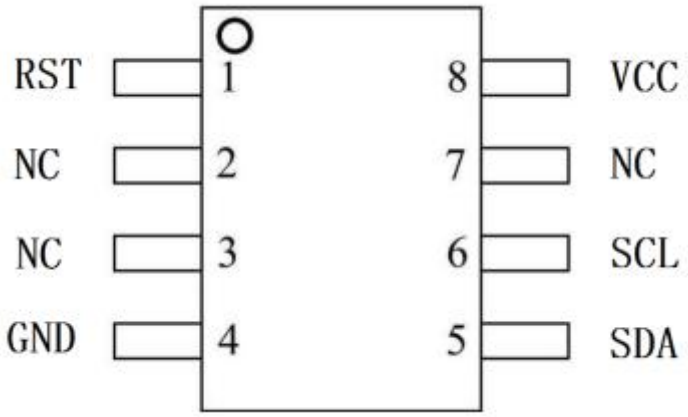


图 1-1： LKT4202U 引脚示意图

1.3 电气特性

工作条件：

符号	说明	条件	最小	典型	最大	单位
VCC	电源电压		1.62		5.5	V
TA	环境温度	---	-40/-25	25	85	℃

VCC 直流特性：

符号	说明	条件	最小	典型	最大	单位
VCC	电源电压		1.62	--	5.5	V
ICCD	峰值电流变化量	Class A, t<400ns, E=20nA.s	--	--	100	mA
		Class B, t<400ns, E=10nA.s	--	--	50	mA
		Class C, t<400ns, E=6nA.s	--	--	30	mA

ICC	正常工作电流，在Flash中执行程序，无PKE/SM4运算	25℃，CPU@48MHz	--	4	6	mA
ICC	Powerdown 电流	TA=25℃	--	0.1	1	uA

电特性：

符号	说明	条件	Min	Max	单位
VIL	Input Low Voltage	VCC=1.62V ~ 5.5V	-0.5	0.3VCC	V
VIH	Input High Voltage	VCC=1.62V ~ 5.5V	0.7VCC	VCC_{max}+0.5	V
V_{HYS}	V_{tz-vtf}	VCC>2V	0.05VCC		V
		VCC<2V	0.1VCC		V
V_{OL-OD}	3mA sink current（@VDD>2V）	F/S mode	0	0.4	V
	3mA sink current（@VDD<2V）	Standard mode	n/a	(n/a)	V
		Fast mode	0	0.2VCC	V
t_{of}	Output fall time from VIH_{min} to VIL_{max} with a bus cap from 10pF to 400pF	Standard mode	---	250	ns
		Fast mode	20+0.1C_b[1]	250	
t_{sp}		Fast mode only	0	50	ns
I_i	Input current each IO pin with an input Voltage between 0.1VCC and 0.9VCC	F/S mode	-10	10	uA
C_i	Cap for each IO pin	F/S mode		10	pF

注1：Cb=capacitance of one bus line in pF.

1.4 产品特性

1.4.1 调试资源

- 32位安全CPU内核
- 全球唯一ID与管理编码

- 支持 IIC 通讯
- 14K 字节密钥文件存储区
- 硬件 DES 协处理器，支持 DES、3DES 算法
- 硬件 AES 协处理器，支持 AES128、AES192、AES256
- 硬件 RSA 协处理器，支持 RSA512-2048bit
- 支持 SHA1、SHA256 算法
- 真随机数发生器

1.4.2 硬件安全特性

- 符合EAL4+安全等级设计要求
- 传感器（电压，时钟，温度，光照）
- 过滤器（防止尖峰/毛刺）
- 独立的内部时钟（独立CLK）
- （SFI）的检测机制
- 被动和主动盾牌
- 胶合逻辑（难以逆转工程师电路）
- 握手电路
- 高密度多层技术
- 具有金属屏蔽防护层，探测到外部攻击后内部数据自毁
- 总线和内存加密
- 虚拟地址（SW =硬件地址！）
- 芯片防篡改设计，唯一序列号
- 硬件错误检测
- 随机数发生器
- 预硅功率分析

1.4.3 软件安全特性

- 内部数据不可读取、拷贝
- 敏感信息进行加密（如：钥匙，别针）
- 双重执行的（如：加密解密核查）
- 校验

- 不能直接访问硬件平台
- 防止缓冲区溢出
- 防止错误的偏移
- 防火墙机制
- 异常计数器
- 执行验证码
- 归零的键和引脚

1.4.4 应用领域

移动支付、电子商务/政务、控制访问、身份识别、控制器，安防监控、游戏机、汽车电子、平板电脑、机顶盒、DVR、路由器、交换机、仪器仪表等各种电子产品终端及应用。

第 2 章 加密方案介绍

2.1 安全认证方案介绍

2.1.1 安全认证方案详解

安全认证方案的实现思路如图 2-1 所示。安全认证是基于国际上通用的对称加密算法（3DES、AES 等）对同一组随机数进行加密后，对结果进行比对判断，基于对称算法的特性，只有认证双方使用相同密钥，才可获得相同加密结果，以此来判别另一方身份是否合法。其安全性更多依赖于对称加密算法自身的安全强度以及密钥的安全存储，使用对称密钥对明文数据加密后再进行线路传输，防止线路攻击，保证无法从线路截取通讯数据攻击获得密钥。安全认证方案实现流程如下，主控 MCU 移植 3DES 或 AES 等对称算法，主控 MCU 与加密芯片端在出厂发行阶段就预置相同的密钥。在运行阶段，MCU 产生随机数 RND 并将其发送给加密芯片，然后两端使用预置的密钥同时对 RND 进行 3DES 加密生成密文 C1 和 C2，最后在 MCU 端比较 C1 与 C2，相同则证明加密芯片身份合法，MCU 程序继续运行；不同则证明加密芯片身份非法，MCU 程序退出运行。

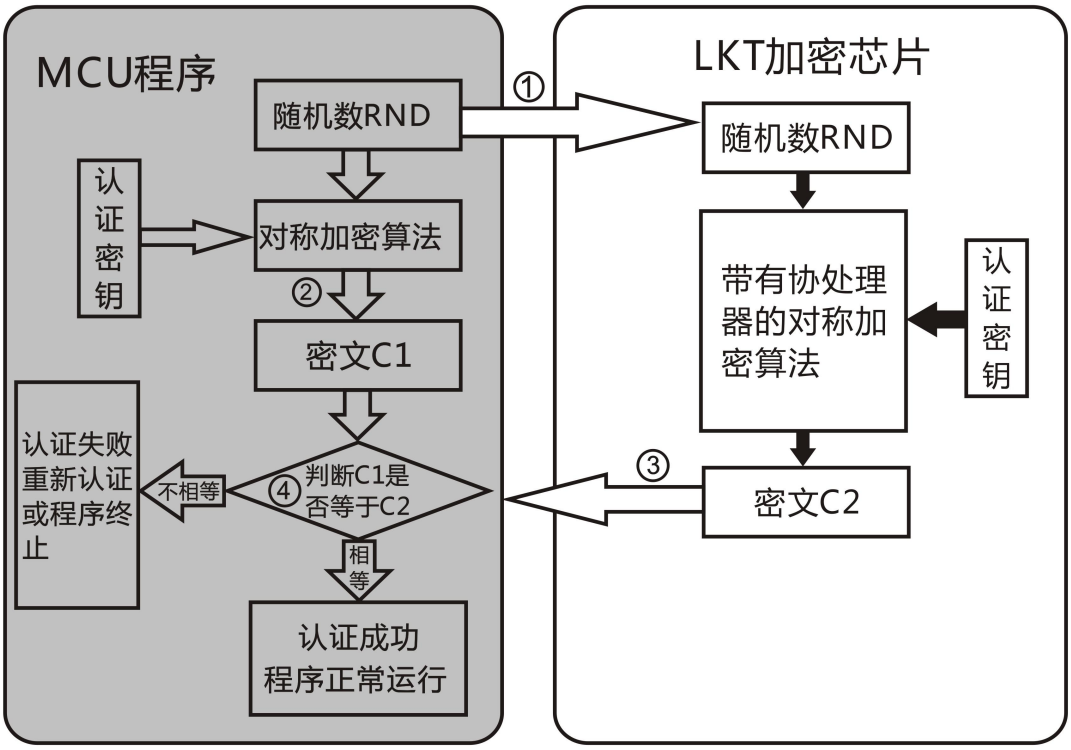


图 2-1：安全认证方案概念

2.1.2 安全认证方案特点

2.1.2.1 方案优点

该方案应用模式固定，调试简单，不需要对主控 MCU 端原有程序做大的改动，也不需要了解加密芯片内部运行流程。因此调试周期极短，研发投入很小。

2.1.2.2 方案缺点

该方案也是目前市面上一些加密芯片的主流加密方案，安全性一般，只能防御非侵入式的线路攻击、重放等破解行为。但是通过对主控 MCU 进行侵入式剖片攻击，可以读出 MCU 端程序进行改写，有效绕过认证对比点。因为 MCU 中的安全认证功能失效，所以在加密芯片没有被破解的情况下，仍可完成盗版行为。

2.1.2.3 注意事项

由于 MCU 端是不安全的，且需要存储一条用于认证的密钥。建议用户不要将该密钥值存储于连续地址（如单个数组中），可以放到内存不同位置，防止被轻易跟踪到。另外，建议用户每次使用认证密钥时，都经过一系列运算后得出密钥，这样真实密钥临时生成于 RAM 中，掉电即丢失，可有效防止防静态分析。

2.2 数据加解密

2.2.1 数据加解密应用介绍

LKT4202U 加密芯片支持 DES/3DES/MAC 等算法功能，用户可以将其作为一个加密计算器使用。将明文或密文送入 LKT4202U 中，即可完成数据加密或者解密操作，进而得到密文或明文数据。因为 LKT4202U 自带硬件协处理器，所以其加解密速度要优于通用 MCU。密钥的安全存储和数据加解密功能已经集成到 LKT4202U 中，用户只需按照规定的 APDU 指令协议与 LKT4202U 完成通讯，即可实现预定功能。

2.2.2 注意事项

密钥的发行和更新环节需要确保线路安全可靠，避免密钥从线路上泄露。在应用过程中若要对密钥进行更新，建议优先考虑以密文加 MAC 的方式进行更新。如果要控制密钥的使用权或修改权，需要在建立密钥的时候就对密钥属性进行设置。详见《LKCOS 智能操作系统参考手册 V3.3》或咨询凌科芯安技术支持人员。

第 3 章 应用文件结构及权限设置

LKT4202U 具有内部文件系统，支持建立 KEY 文件、二进制文件、记录文件等应用结构。用户可根据项目的实际需求，有选择的建立使用。因为应用文件结构的创建、使用、权限的管理等内容非常细致复杂，此章节不做详细解析，具体指令应用和权限解析详见开发套件中的《LKCOS 智能操作系统参考手册 V3.3》。

3.1 文件结构

加密芯片出厂默认为空结构，必须建立基本文件结构才可使用。基本文件结构如图 3-1 所示。其中红色字体为必须建立的基本文件结构；黑色字体为扩展应用结构。下面分别介绍各种文件结构的作用。

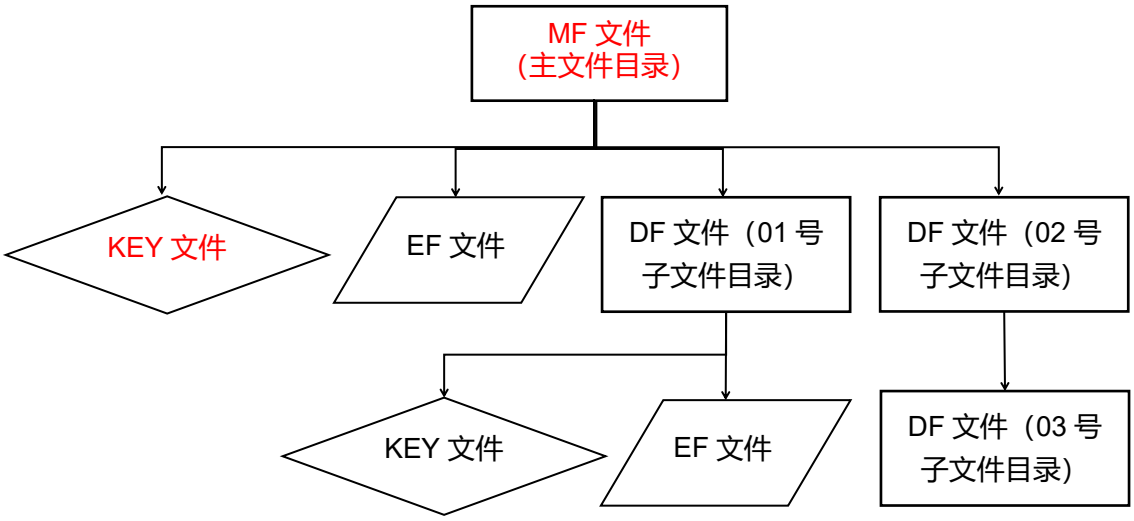


图 3-1：基本文件结构

3.1.1 MF 文件

MF 文件是根目录，有且只有一个，一经建立不能擦除或更改。

3.1.2 DF 文件

DF 文件是 MF 下的子目录。每个 DF 下还可继续建立下一级 DF 目录。

3.1.3 EF 文件

EF 文件是 MF 文件或者 DF 文件下面的基本文件。EF 文件分为安全基本文件和工作基本文件。

3.1.3.1 安全基本文件（Key 文件）

安全基本文件简称 Key 文件，存储用于用户识别和与加密有关的密钥数据。在每个 MF 或 DF 下，有且只能存在一个 Key 文件。当 MF 或 DF 建立成功后，必须先建立 Key 文件，再进行其他文件结构的创建和写入密钥等操作。

3.1.3.2 工作基本文件（EF 文件）

工作基本文件包括二进制文件、定长记录文件、循环记录文件等。二进制文件是以字节为单位访问的文件，支持从任意位置访问任意长度的数据，前提是不超出文件大小范围。定长记录文件是以记录为访问单位的文件，可由多条记录组成，每条记录的长度是固定一致的，一次读出整条记录内容。其他基本文件类型介绍详见《LKCOS 智能操作系统参考手册 V3.3》。

3.2 权限设置

3.2.1 EF 文件读写权限

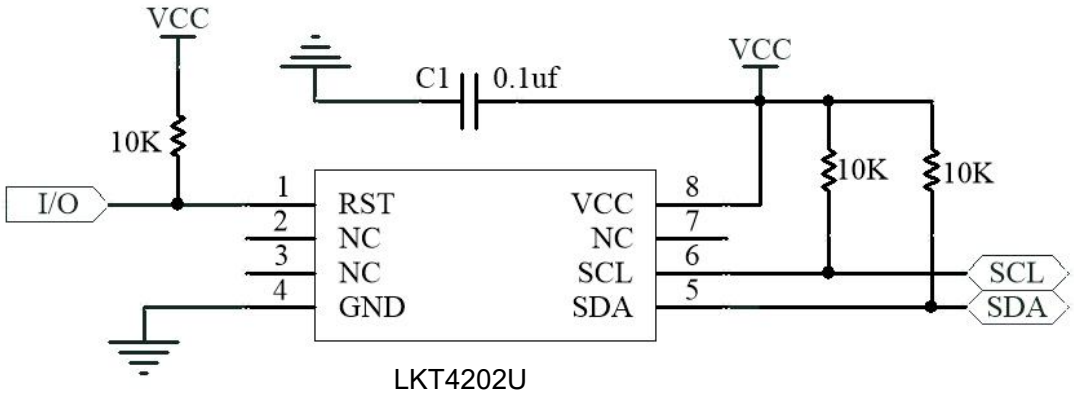
EF 文件用于存储数据。在建立 EF 文件的时候，可以对文件的读写权进行设置。避免文件内部的数据被非法读取或篡改。

3.2.2 密钥更新使用权限

向 Key 文件内写入密钥的时候，可以在写入指令中对密钥的更新和使用权进行设置。避免密钥被非法使用或篡改。

第 4 章 通讯调试说明

4.1 通讯电路



LKT4202U

4.2 通讯时序

4.2.1 复位时序

电源正常供给后，当 LKT4202U 的 RST 引脚出现由低到高的时序后，LKT4202U 将执行复位操作，时序如图 4-1 所示。

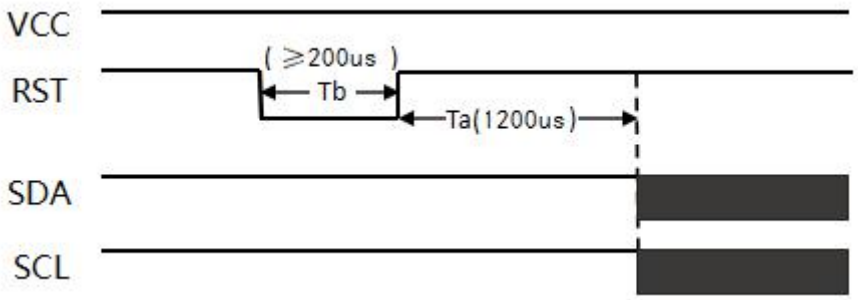
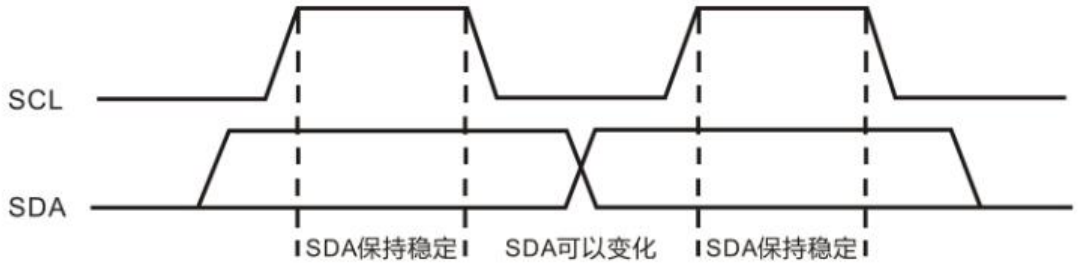


图 4-1： 复位时序

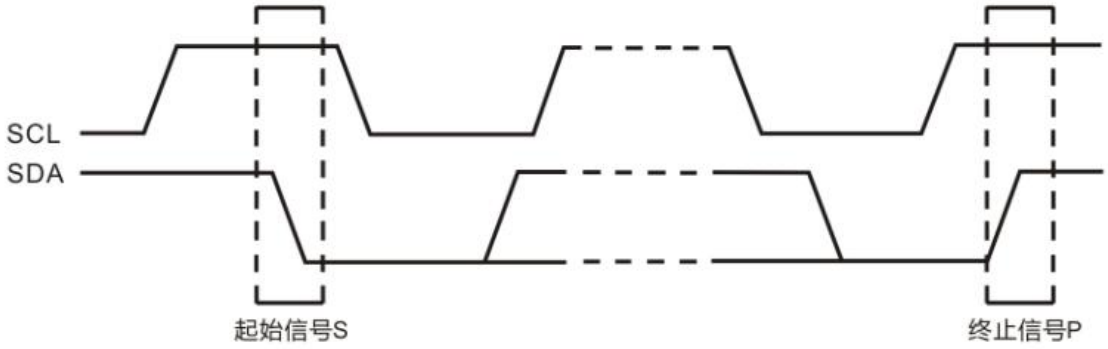
4.2.2 IIC 通讯时序

（1） 数据位的有效性规定



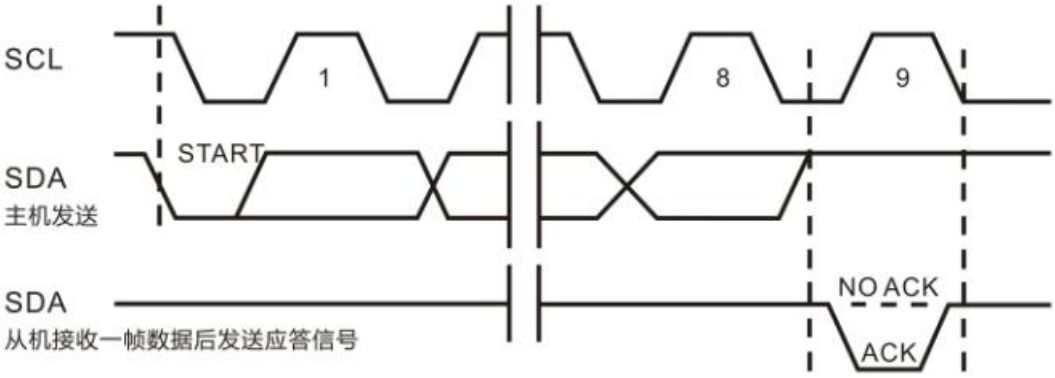
I2C 总线进行数据传送时，时钟信号为高电平期间，数据线上的数据必须保持稳定，只有在时钟线上的信号为低电平期间，数据线上的高电平或低电平状态才允许变化。

（2）起始信号和停止信号



SCL 线为高电平期间，SDA 线由高电平向低电平的变化表示起始信号；SCL 线为高电平期间，SDA 线由低电平向高电平的变化表示终止信号。起始和终止信号都是由主机发出的，在起始信号产生后，总线就处于被占用的状态；在终止信号产生后，总线就处于空闲状态。

（3） I2C 总线应答（ACK）时序图



每一个字节必须保证是 8 位长度。数据传送时，先传送最高位（MSB），每一个被传送的字节后面都必须跟随一位应答位（即一帧共有 9 位）。

第 5 章 芯片封装

LKT4202U 标准封装为 SOP8，如图 7-1 所示。也支持定制其他封装形式。

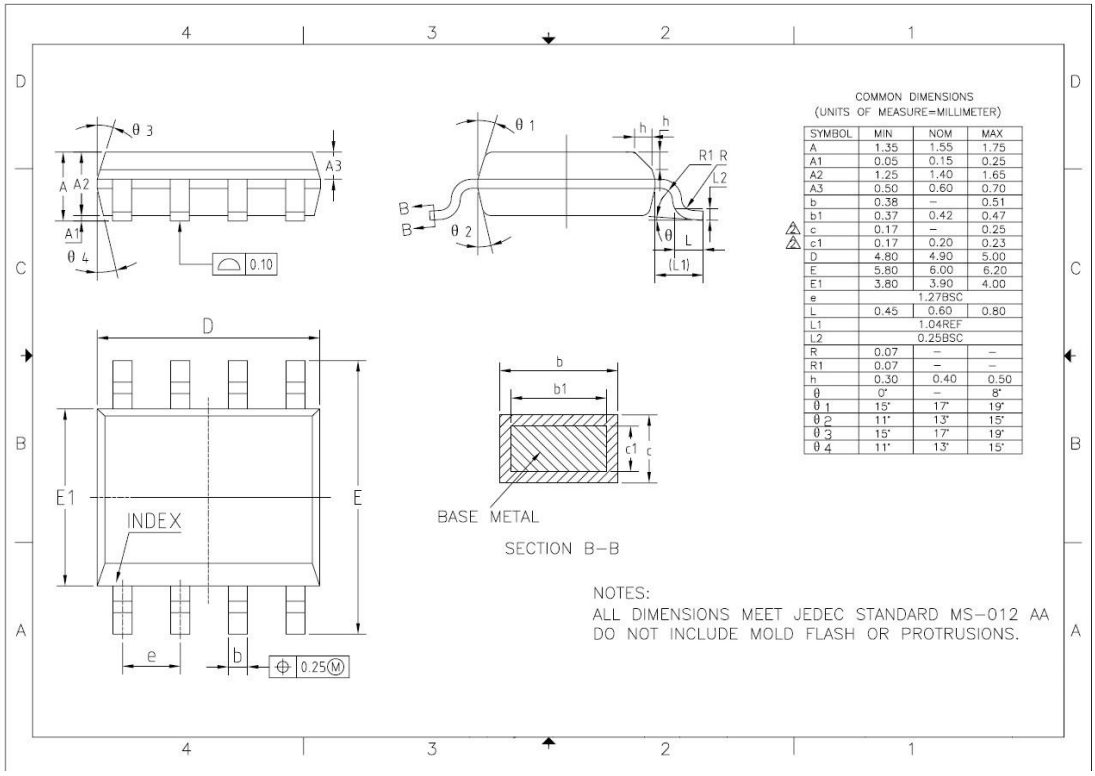


图 5-1： SOP8 封装图