LKT4304　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 LKT4304 芯片硬件特性

1.1 芯片参数

CPU

- 高性能32位安全CPU内核
- 32位指令系统

片上存储

- 128K-Bytes 程序存储区
- 64K-Bytes NVM数据存储区
- 32K-Bytes RAM
- 64K-Bytes 文件密钥区

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
- 硬件DES/TDES协处理器
- 异常情况探测
- 内存数据动态加密
- FLASH存储区加密
- 优化安全布局

通讯接口

- SPI接口x 1
- I2C接口x 1

奇偶校验/ CRC计算器

- 8 / 16 / 32位奇偶校验
- CRC-16/32 计算器

可控GPIO

- GPIO：最多3个

复位

- 上电冷复位
- 热复位

操控特性

- 单电源：3.3V
- 工作温度：- 40 ℃ ~+ 85℃
- 最大工作电流：30mA
- 最大待机电流：200uA

1.2 引脚定义

表1-1： LKT4304 引脚说明

引脚序号	引脚名称	功能描述	引脚类型
1	SCK/SDA	SPI_CLK 或 IIC_SDA	输入/输出
2	GND	地	
3	SS	SPI_SS	输入
4	MISO	SPI_MISO	输入/输出
5	MOSI/SCL	SPI_MOSI 或 IIC_SCL	输入/输出
6	RST	复位	输入
7	SPI_BUSY	SPI_BUSY	输出
8	VCC	电源 3.3V	

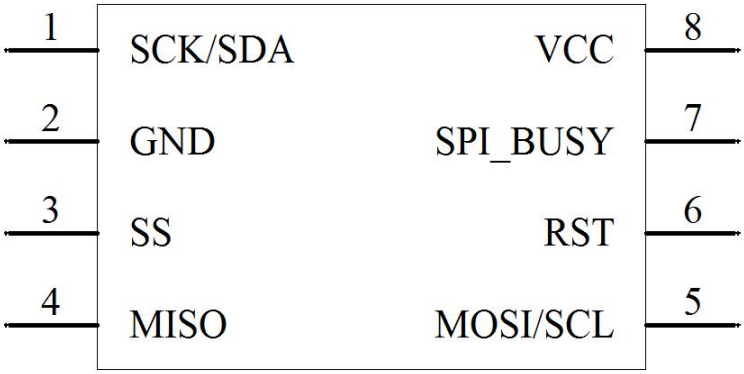


图1-1： LKT4304 引脚说明

1.3 电气特性

工作条件

符号	说明	条件	数值	单位
VCC	工作电压		2.97~3.63	V
Top	工作温度		-40~85	℃
Tstore	存储温度		-40~150	℃

电压及电流

符号	说明	条件	最小	典型	最大	单位
VCC	工作电压	工作模式	2.97	3.3	3.63	V
Icc	工作电流	工作模式(@90MHz)			30	mA
IccS	待机电流	工作模式，待机状态，VCC=3.3V			200	uA

1.4 芯片安全特性

1.4.1 内部调试资源

- 采用 32 位安全芯片内核，内置 32 位加密操作系统
- 全球唯一硬件 ID 与管理编码
- 具有 128K 字节超大用户程序下载空间
- 64K 字节可定义安全性 NVM 数据存储区
- 32K 字节程序 RAM
- 64K 字节文件密钥区
- 支持单精度浮点运算
- 具有丰富的系统调用和开发接口，支持多种数学运算
- 硬件 AES/DES/TDES/RSA/ECC（可定制）等协处理器

1.4.2 硬件安全特性

- 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
- （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
- 真正的随机数发生器（RNG）
- 噪音的产生（对边信道攻击）
- 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（钥匙，别针）
- 双重执行的（如加密解密核查）

- 校验
- 验证程序流
- 不可预知的时序（如随机 NOP）
- 不能直接访问硬件平台，HAL（汇编），C
- 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 算法移植方案介绍

2.1.1 算法移植方案详解

LKT4304 是凌科芯安科技（北京）有限公司行业内独家开发的以 32 位安全处理器为基础的具有高性能高安全性的加密产品（以下简称加密芯片），算法移植方案具备方法型发明专利，专利号“ZL 2012 1 0546174.9”。用户将 MCU 程序中一部分关键算法移植到加密芯片中运行，如图 2-1 中所示，第一步先将代码 2 移植到加密芯片中。用户采用标准 C 语言编写代码，通过 C 编译器编译并下载到加密芯片中。在实际运行中，通过调用函数方式运行加密芯片内的程序段，获得运行结果，并以此结果作为用户程序进一步运行的输入数据。因此加密芯片成为了产品的一部分，而算法在加密芯片内部运算，盗版商无法破解，从根本上杜绝了程序被破解的可能。

MCU 程序分为两个部分：一部分是在 MCU 中，另一部分在加密芯片中。当需要用到加密芯片中的算法时 MCU 向其发送指令，加密芯片根据指令在内部运行程序并返回结果给 MCU。

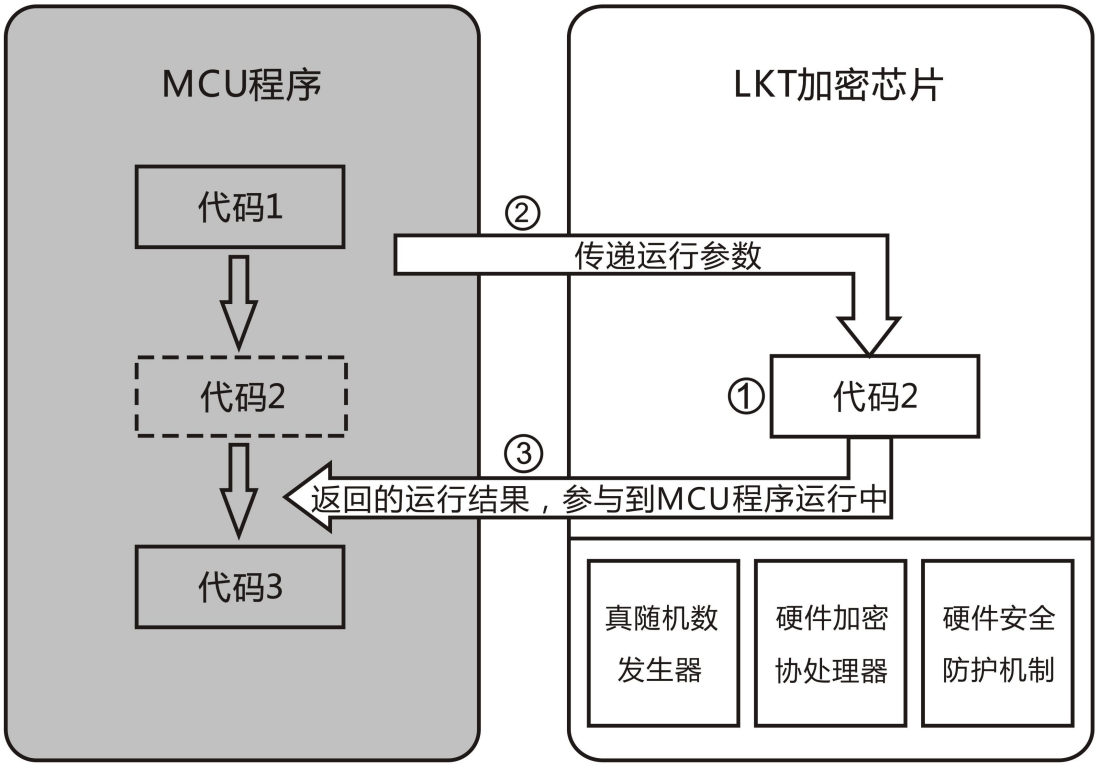


图 2-1：算法移植概念

2.1.2 算法移植方案特点

2.1.2.1 方案优点

最大限度的发挥了加密芯片的安全特性，让加密芯片与主控 MCU 的功能结合使用，MCU 核心代码分别在 MCU 和加密芯片中存储运行，单独破解 MCU 无法获取全部核心关键代码，以此提升整个系统的安全等级，让系统安全达到了质的飞跃。让盗版商和破解团队无从下手分析，从而无法盗版产品。

2.1.2.2 方案缺点

因为需要对加密芯片算法结构与运行流程有清晰的了解，因此算法调试周期相对较长；加密芯片为了防止破解分析不支持在线调试，只能在运行结束后将过程数据打印输出进行分析。

2.1.2.3 注意事项

选择移植的算法时，要兼顾考虑实时性、算法自身复杂度等问题。不要将整个 MCU 程序都移植到加密芯片中，也不要选择实时性要求过高的算法，同时也要保证算法运行结果是非线性的，不会被轻易分析出来。建议如下：

输入输出数据不能是一成不变的。

输入输出之间不能是线性变化的。

输出结果返回到 MCU 中，建议作为程序下一步运算的重要参数。

输入输出数据的乱序迷惑处理，同时在输入输出数据中加入随机数增大分析难度。

线路数据最好以密文形式传递，防止被线路跟踪。

2.2 对比认证方案介绍

2.2.1 对比认证方案详解

对比认证方案的实现思路如图 2-2 所示。对比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。对比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一组密钥。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。

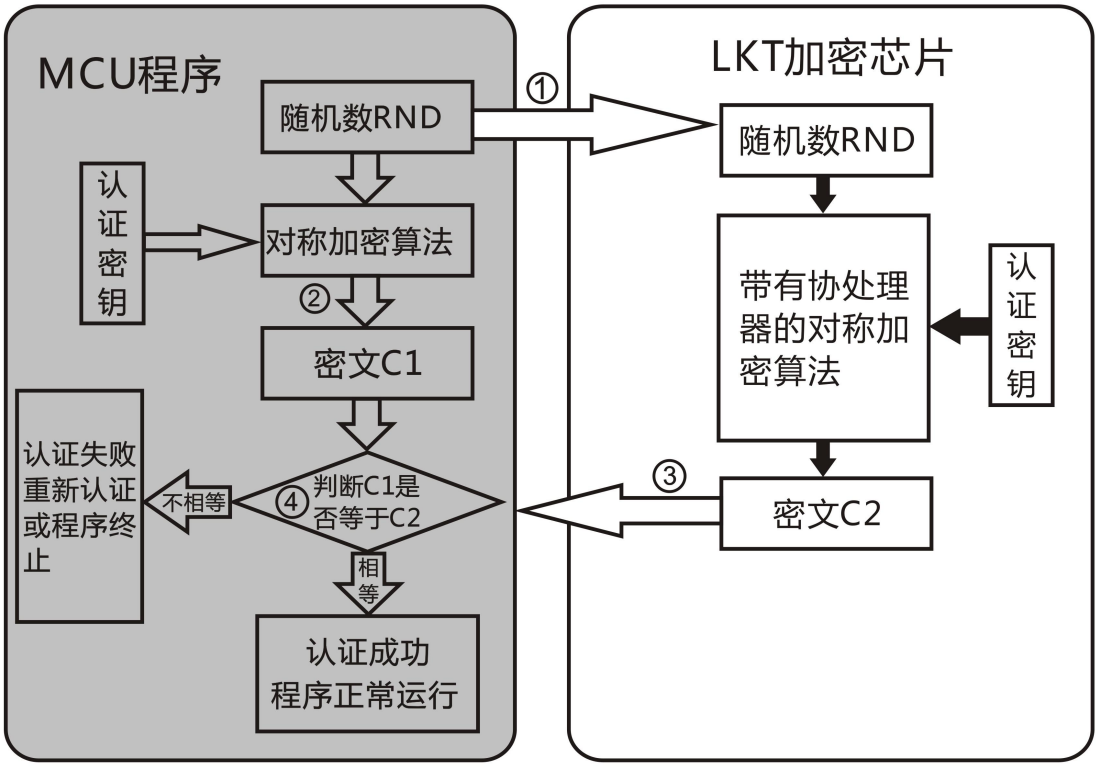


图 2-2： 对比认证方案概念

2.2.2 对比认证方案特点

2.2.2.1 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。

2.2.2.2 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 中的对比认证功能失效，所以在加密芯片没有被破解的情况下，仍可完成盗版行为。

2.2.2.3 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。

2.3 参数保护方案介绍

2.3.1 参数保护方案详解

参数保护方案的实现思路如图 2-3 所示。用户可以把 MCU 中的一部分关键参数移植到加密芯片中存储。在实际运行中，MCU 发送读回参数指令和随机数到加密芯片端，后者也产生一组随机数，利用这两组随机数作为输入数据，结合预置的密钥对预存的关键参数进行加密生成密文，然后将密文参数和加密芯片产生的随机数回传到 MCU 端。此时，MCU 使用预置的解密密钥对密文参数进行解密操作，还原出关键参数 M，并将 M 作为程序进一步运行的输入数据参与到后续运行中。因为加密芯片存储了 MCU 中的关键数据，因此也成了产品的一部分，只对 MCU 进行破解攻击，不能获取到完整的参数，而缺失的关键参数存储于加密芯片中，可有效防止破解，从而起到了有效防护。加密芯片的引入，虽然无法阻止盗版商对 MCU 程序进行破解攻击，但通过对 MCU 原有关键参数的有效保护，杜绝了盗版商的抄板行为。

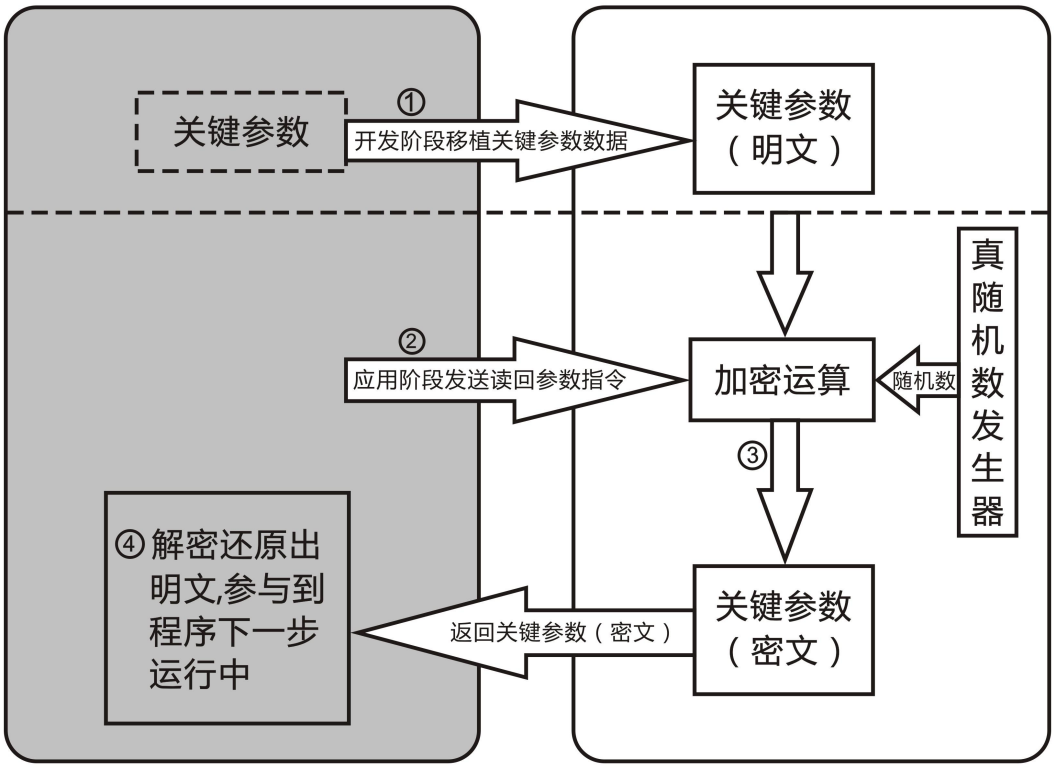


图 2-3：参数保护方案概念

2.3.2 参数保护方案特点

2.3.2.1 方案优点

该方案应用模式支持用户自定义，包括加密算法的选择和加密模式的设定。安全性仅次于算法移植方案，高于市面上常见的对比认证方案，调试简单，不需要对主控 MCU 端原有程序做太大的改动，虽然需要了解加密芯片内部运行流程，但不需要做太多编程改动，只需了解基本的底层接口应用方式。调试周期介于算法移植和对比认证之间，研发投入相对较小。盗版商没法直接找到比对点，程序执行中没有绝对的对错，而是会影响运行效果。综合比较，其开发难度小于算法移植方案，安全等级高于对比认证。该方案适用于实时性要求高，MCU 找不到合适的算法进行移植，但又需要高安全防护的项目。

2.3.2.2 方案缺点

因为没有像对比认证方案那样在 MCU 端出现比较明显的比对点，所以该方案安全性相较对比认证有所提升，可以防御非侵入式的线路攻击、重放等破解行为。但无法达到算法移植方案那样高的安全等级。

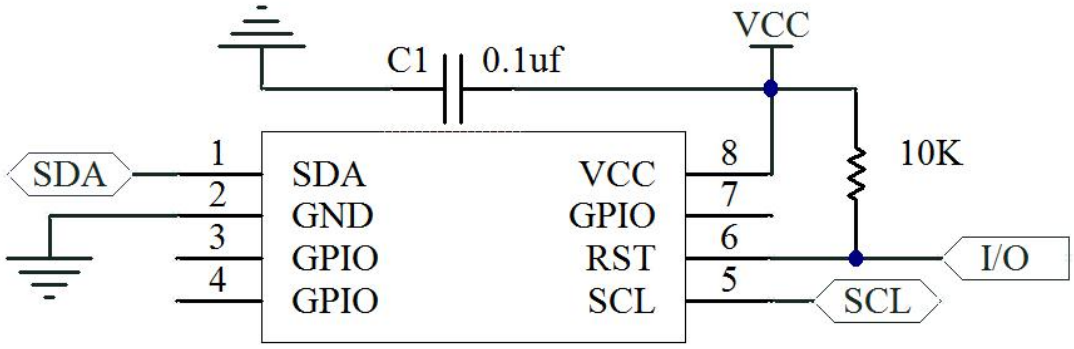
2.3.2.3 注意事项

存储于加密芯片中的关键参数可以保证存储安全，当经线路传回到 MCU 端时，要进行线路加扰处理，MCU 和加密芯片端都产生随机数并参与到加密芯片内部关键数据的加密过程中，可保证线路数据以随机密文方式传输，切忌使用固定的明文或者固定的密文进行传输。由于 MCU 端是不安全的，且需要存储一条用于解密还原重要参数的密钥，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。

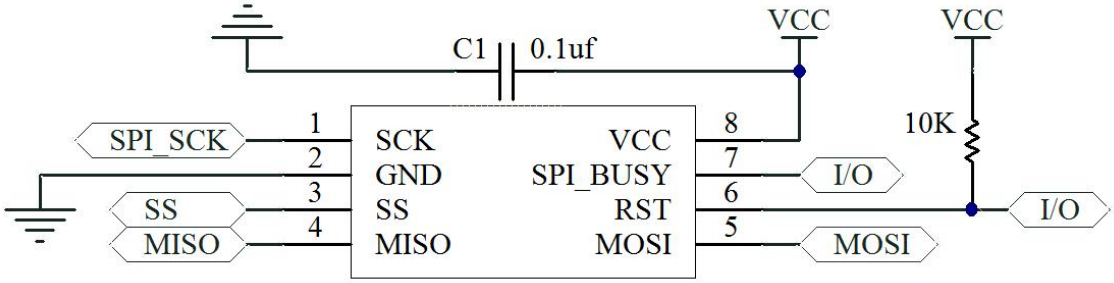
第 3 章 通讯调试说明

3.1 通讯电路

3.1.1 IIC 电路



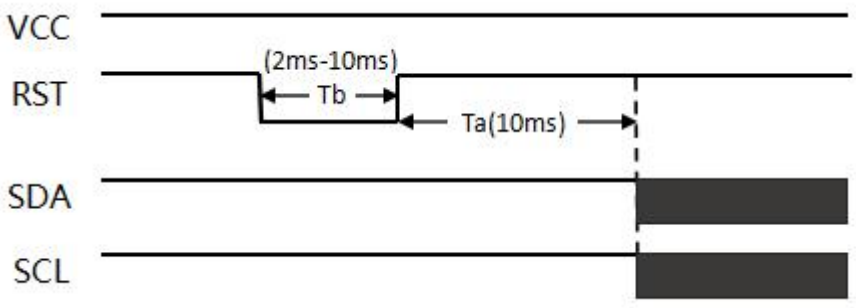
3.1.2 SPI 电路



3.2 通讯时序

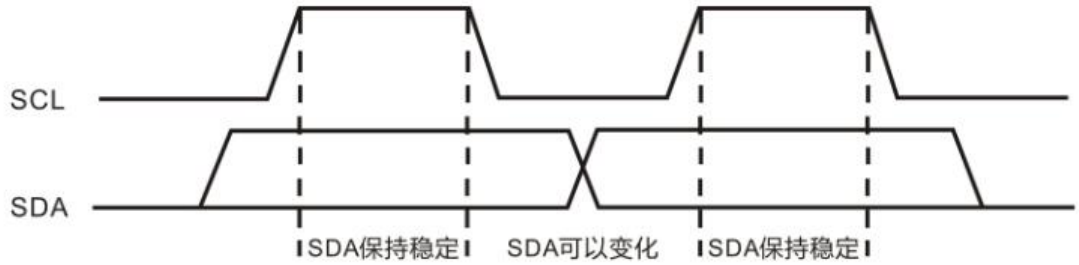
3.2.1 IIC 复位时序

电源正常供给后，将 LKT4304 的 RST 引脚拉低 2~10ms 后拉高，LKT4304 将进行复位操作，复位操作 10ms 内完成。



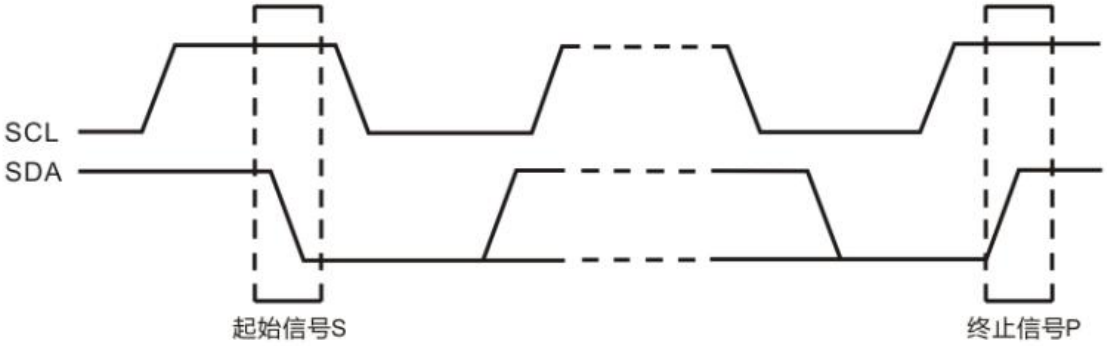
3.2.2 IIC 通讯时序

（1） 数据位的有效性规定



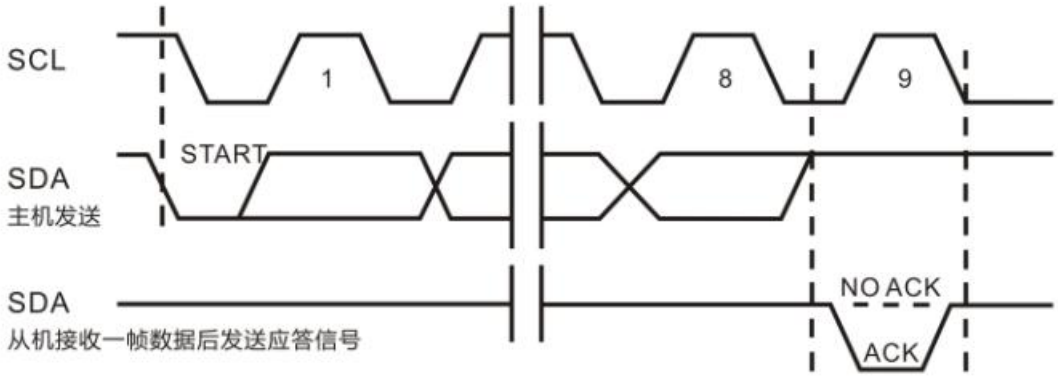
I2C 总线进行数据传送时，时钟信号为高电平期间，数据线上的数据必须保持稳定，只有在时钟线上的信号为低电平期间，数据线上的高电平或低电平状态才允许变化。

（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

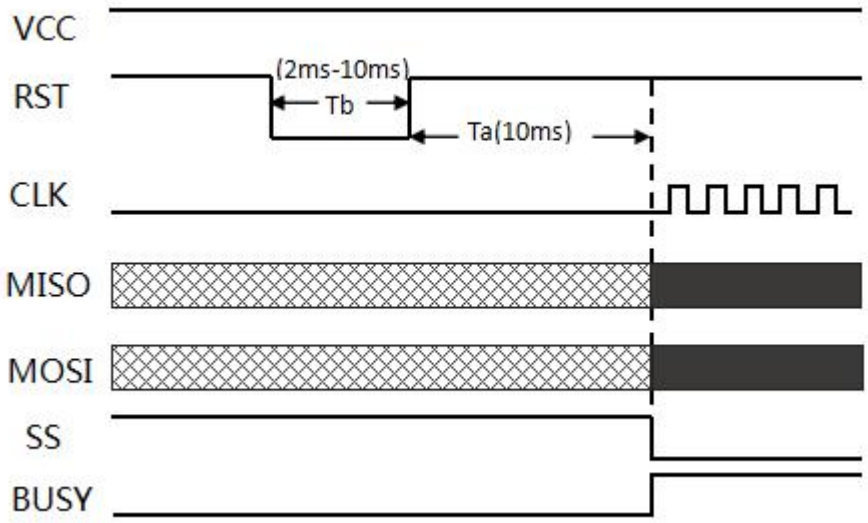


每一个字节必须保证是 8 位长度。数据传送时，先传送最高位（MSB），每一个被传送的字节后面都必须跟随一位应答位（即一帧共有 9 位）。

3.2.3 SPI 复位时序

电源正常供给后，将 LKT4304 的 RST 引脚拉低 2~10ms 后拉高，LKT4304 将进行复位操作，复位操作 10ms 内完成。

复位时序：



第 4 章 芯片封装

LKT4304 标准封装为 SOP8，如图 6-1 所示。也支持定制其他封装形式。

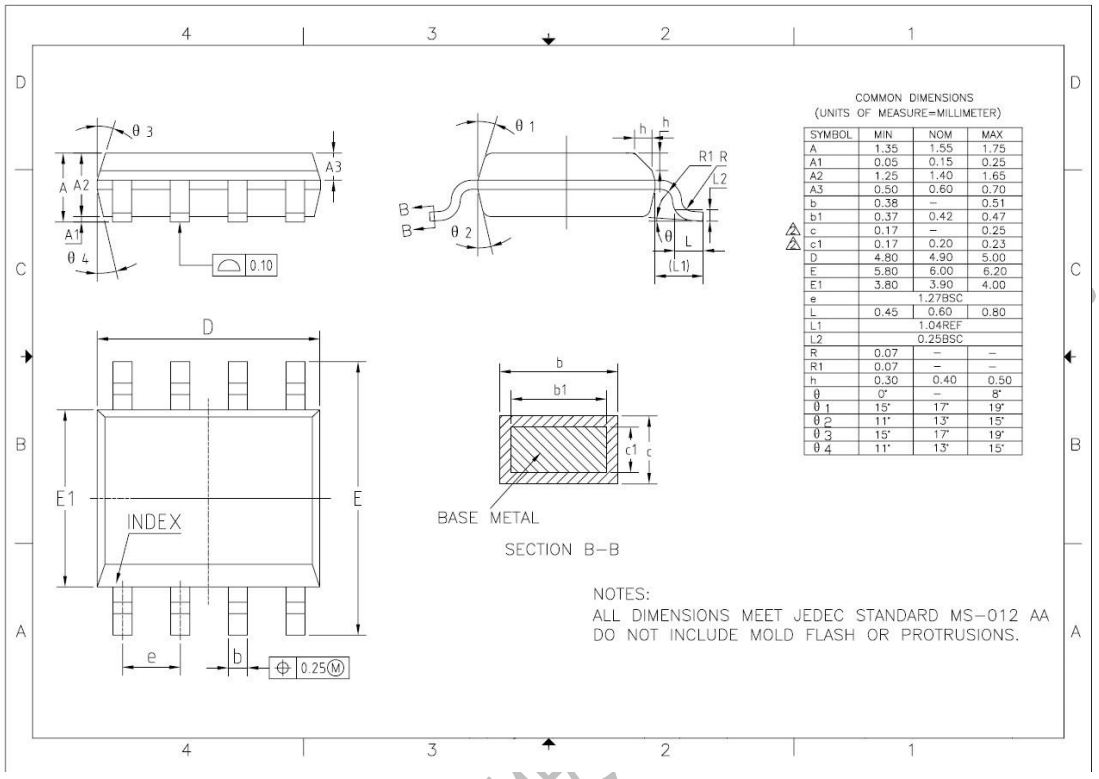


图 4-1： SOP8 封装图