LKT4304 32 位加密芯片

数据手册

仅限凌科芯安客户使用，未经允许请勿转载

凌科芯安科技（北京）有限公司

版本记录

当前版本		V1.1.0	2022.8.11
原始版本		V1.0.0	2018.10.10
升级说明			
升级日期	版本号	新增内容	修改内容
2022.8.11	V1.1.0		修改描述性语言

仅限凌科芯安客户使用，未经允许请勿转载

联系凌科芯安

公司名称：凌科芯安科技（北京）有限公司
办公地点：北京市石景山区古城西街 255 号院 1 号楼中海大厦 B 座 1301
电话　　：010-68864300
传真　　：010-68864300-604

仅限凌科芯安客户使用，未经允许请勿转载

目　录

仅限凌科芯安客户使用，未经允许请勿转载

第 1 章 硬件特性

1.1 芯片特性

CPU

- 高性能 32 位安全 CPU 内核
- CPU 内频最高 90MHz

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
- 小端模式

Flash 寿命

- 不低于 10 万次擦写次数或 10 年有效存储
- 扇区大小 512-Bytes
- 4 字节写操作

数据安全机制

- 硬件真随机数发生器
- 唯一硬件 ID 号
- DES/TDES 硬件协处理器
- RSA 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

I2C 控制器

- I2C 从模式
- 支持硬件 IIC 总线协议
- 通讯标准 100kbps，快速 400kbps

CRC 计算器

- CRC-16 计算器

复位

- 上电冷复位
- 热复位

通讯接口

- SPI 接口 x 1
- I2C 接口 x 1

操控特性

- 单电源 3.3V
- 工作温度：－40 ℃ ~ +85℃
- 最大工作电流 10mA
- 不支持低功耗模式
- ESD 保护大于 4000V

仅限凌科芯安客户使用，未经允许请勿转载

1.2 引脚定义

表 1-1　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_CS	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	

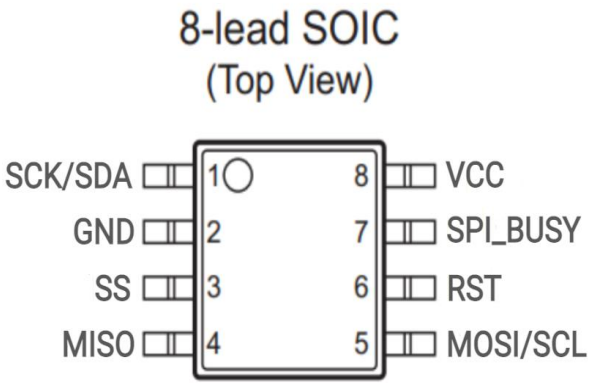


图 1-1　引脚说明

1.3 接口电路

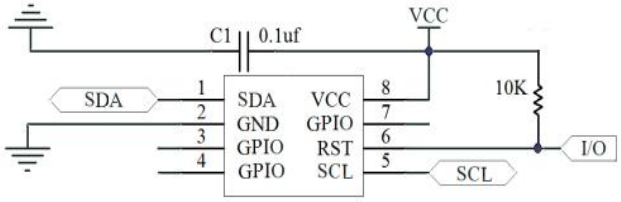


图 1-3　IIC 接口电路

仅限凌科芯安客户评估测试使用，未经允许请勿转载

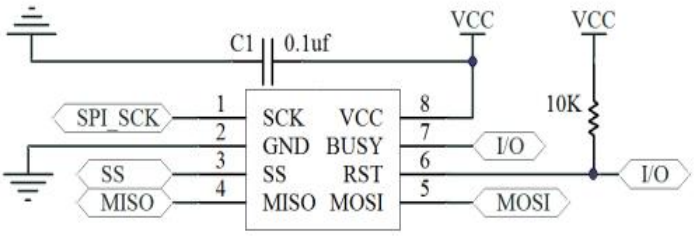


图 1-4　SPI 接口电路

1.4 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
TA	工作温度		-40~85	℃
TSTG	存储温度		-40~150	℃

DC 特性：

符号	说明	条件	最小	典型	最大	单位
VCC	工作电压	3.3V	2.97	3.3	3.63	V
ICC	工作电流	@内频 90MHz				mA

电特性：

符号	说明	单位	最小	典型	最大
VIH	Input High Voltage	V	2.0		VCC+0.3
VIL	Input Low Voltage	V	-0.3		0.8
VHYS	Schmitt trigger hysteresis	V	3.3	0.1xVCC	
IOZ	Tri-State output leakage Current	uA			±10
IL	Input Leakage Current	uA			±10
VOL	Output Low Voltage	V			0.4
VOH	Output High Voltage	V	2.4		

仅限凌科芯安客户使用，未经允许请勿转载

第 2 章 时序说明

2.1 复位时序

芯片为低电平复位，高电平工作。当 RST 引脚拉低后芯片进入复位状态，RST 拉高后芯片开始执行初始化操作，延时 5ms 后 MCU 端可通过 IIC/SPI 接口向加密芯片发送指令，如下图所示：

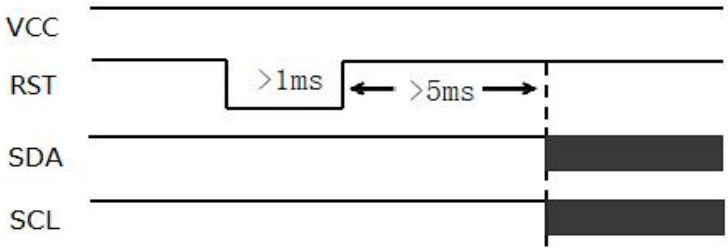


图 2-1： IIC 复位时序

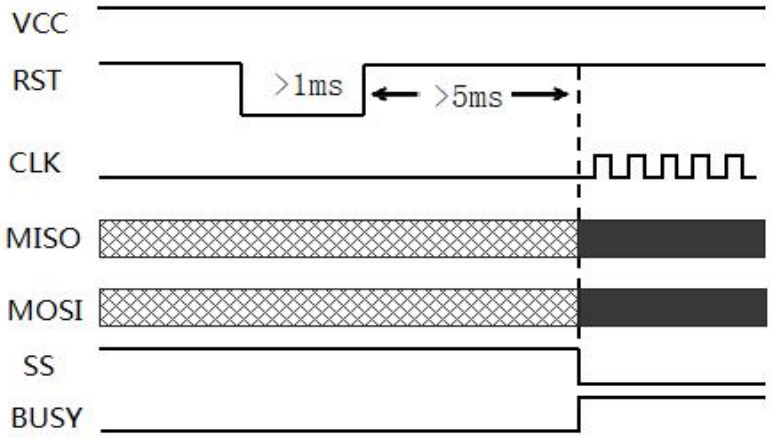
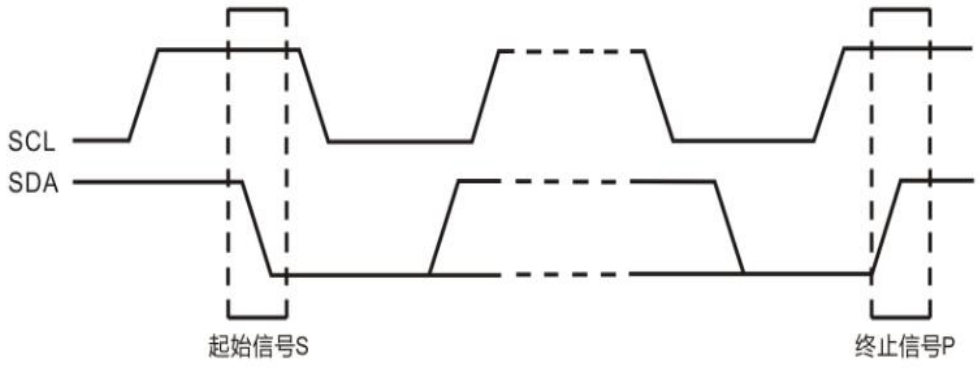


图 2-2： SPI 复位时序

2.2 I2C 时序

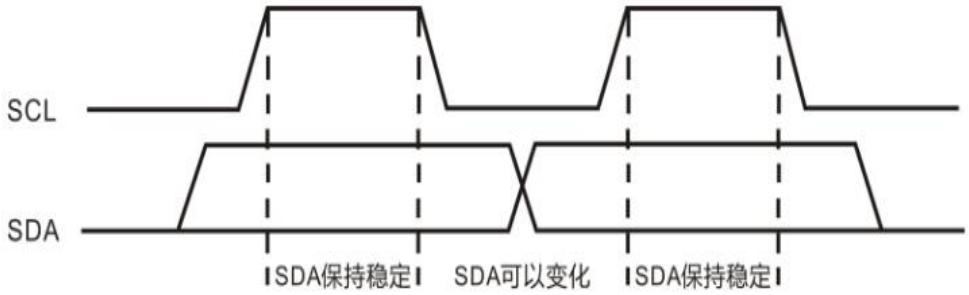
（1）起始信号和停止信号



仅供凌科芯安产品设计请勿转载

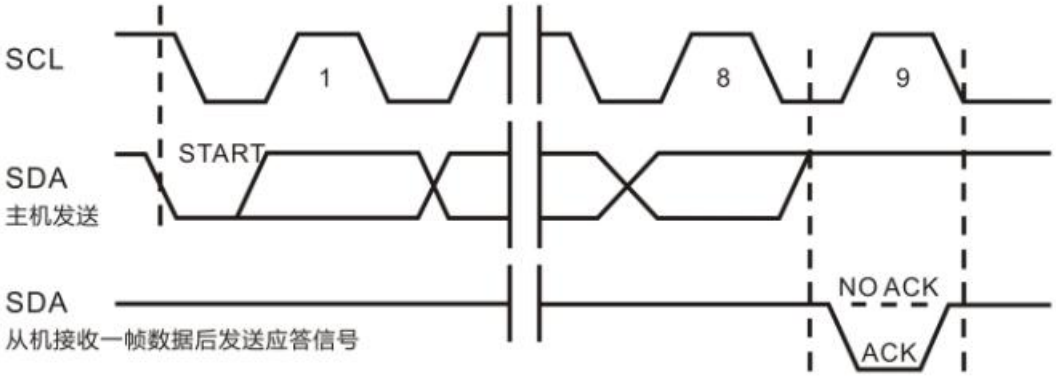
SCL 线为高电平期间，SDA 线由高电平向低电平的变化表示起始信号；SCL 线为高电平期间，SDA 线由低电平向高电平的变化表示终止信号。起始和终止信号都是由主机发出的，在起始信号产生后，总线就处于被占用的状态；在终止信号产生后，总线就处于空闲状态。

（2）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。

（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）。

2.3 SPI 时序

时序说明：

LKT4304 需作为 SPI 从机，上位机端作为 SPI 主机。

当 LKT4304 芯片运行异常时，可对其进行硬件复位操作。

硬件复位操作流程是将芯片第 6 引脚 RST 拉高后，一直保持为高电平状态。

主机 SPI 设置成 CKPOL = 0 ；CKPHA = 0；

BUSY 引脚为高电平，允许 SPI 主设备发送数据。

SPI 通讯时序如下图 2-3 所示：

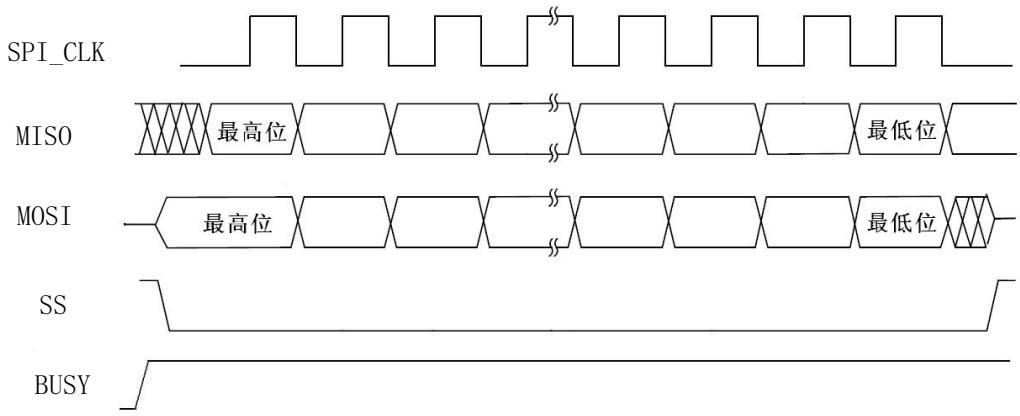


图 2-3： SPI 接收时序

BUSY 为 SPI 请求信号。当 BUSY 拉低时允许 SPI 主设备读取数据，此时 SPI 主机端将 SS 拉低，SPI_CLK 产生时钟。LKT4304 发送时序如图 2-4 所示。

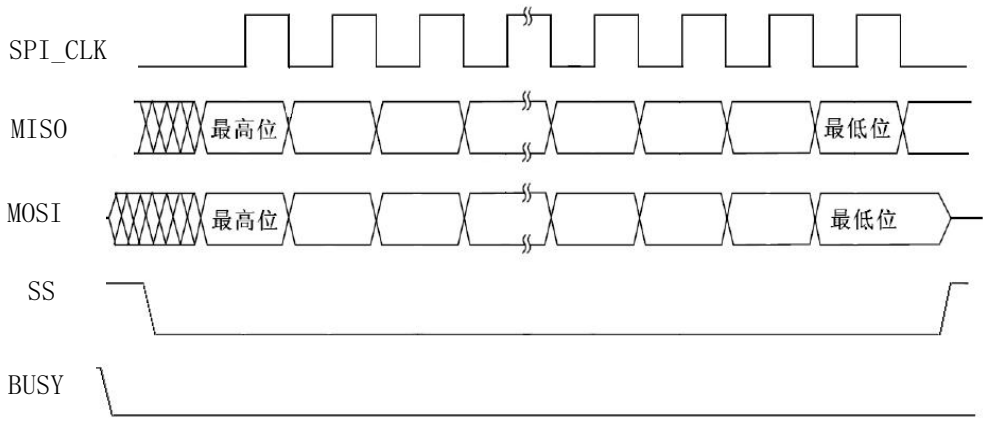


图 2-4：SPI 发送时序

仅限凌科芯安内部使用 未经许可 禁止转载

第 3 章 指令集

我司 LKT4304 支持如下指令，具体指令使用说明参看芯片开发手册。

缩写	CLA	INS	指令功能	说明
CallUserApp	80	08	调用应用层代码功能指令	具体调用芯片实现何种功能由传入的数据域内容决定
Random	00	84	从加密芯片获取随机数	
SetPrarmData	80	CC	设置芯片运行参数	P1=00，P2=02 时为接口设置指令
VerifyCmd	F0	F6	加密芯片下载代码时的验证类指令	1.P1=00，P2=00 时验证算法下载口令 2.P1=00，P2=01 时获取算法压缩码 3.P1=00，P2=02 时验证算法注册码 4.P1=80，P2=00 时设置芯片密文下载时的解密密钥
DownloadCode	F0(F4)	F4	下载应用程序代码到加密芯片	1.CLA=F0 时为明文方式写操作 2.CLA=F4 时为密文方式写操作

仅限凌科芯安客户使用，未经许可禁止转载

第 4 章 芯片封装

标准封装为 SOP8，如图 4-1 所示。同时支持定制其他封装形式。

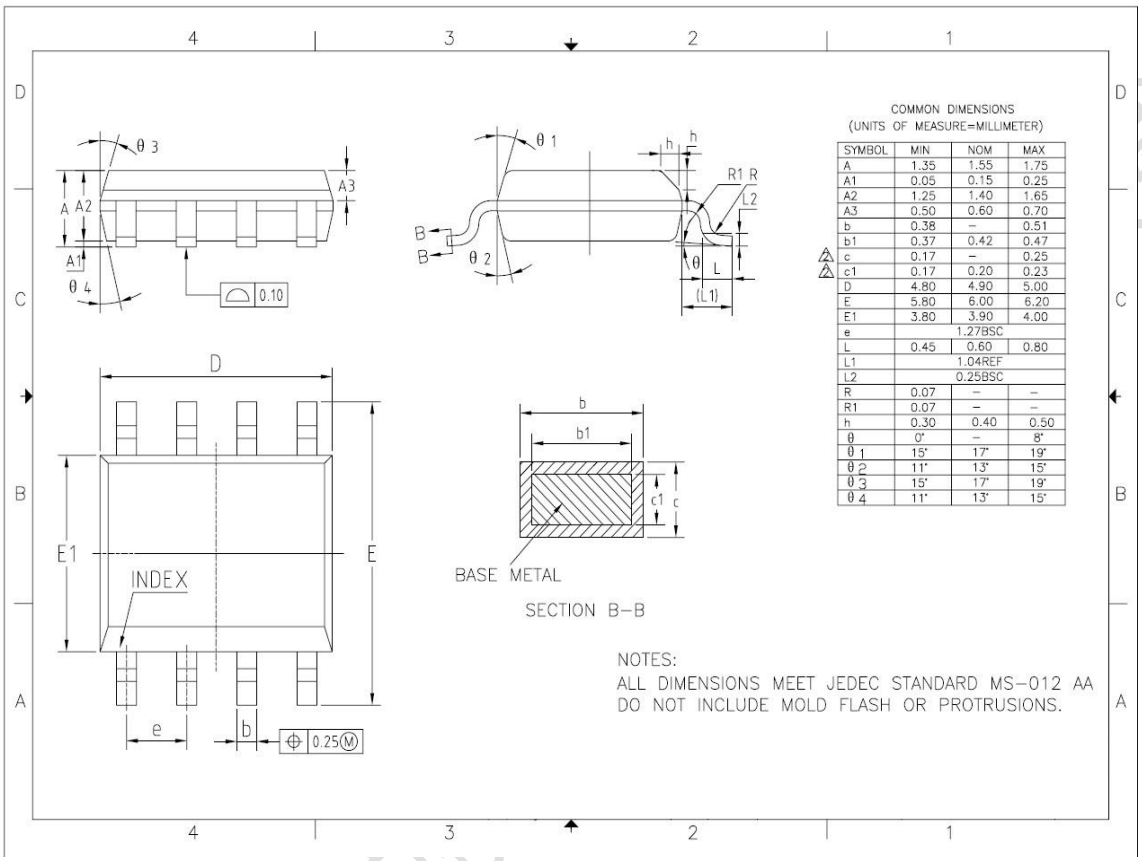


图 4-1 SOP8 封装图

仅限凌科芯安客户