LCS2110R　32 位加密芯片

开发手册

凌科芯安科技（北京）有限公司

版本记录

当前版本	V1.1	2022.06.20
原始版本	V1.0.0	2021.11.23

升级说明			
升级日期	版本号	新增内容	修改内容
2022.06.20	V1.1	Sot23-5 封装及说明	

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

目　录

第 1 章 LCS2110R 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25MHz

片上存储

- 16K-Bytes 密钥文件存储区

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
- 唯一硬件ID号
- 全内存加密
- 256字节安全（只读）和256字节的不可擦Flash区
- 如果检测到异常电压或异常频率，复位操作有效

加密协处理器

- 模幂加速器

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

奇偶校验/ CRC计算器

- 8 / 16 / 32位奇偶校验
- CRC-16/32 计算器

复位

- 上电冷复位
- 热复位

操控特性

- 单电源 3.0V ~ 5.5V
- 工作温度: – 40 ℃ ~+ 85℃
- 正常工作电流 5mA
- 关断模式电流 0.1uA
- ESD保护大于4000V

1.2 引脚定义

表1-1： LCS2110R SOP8引脚说明

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

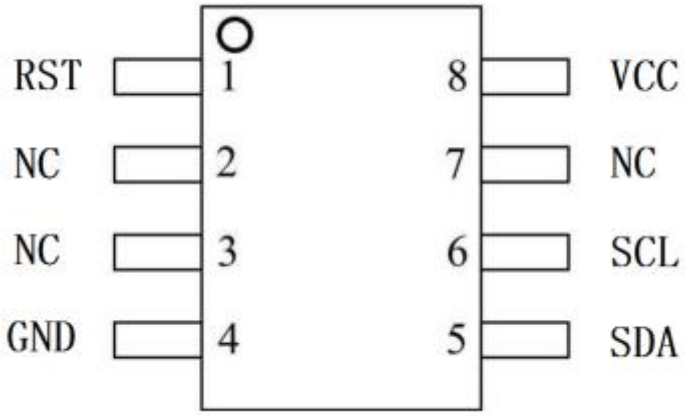


图 1-1： LCS2110R SOP8 引脚说明

表1-2： LCS2110R　SOT23-5 引脚说明

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

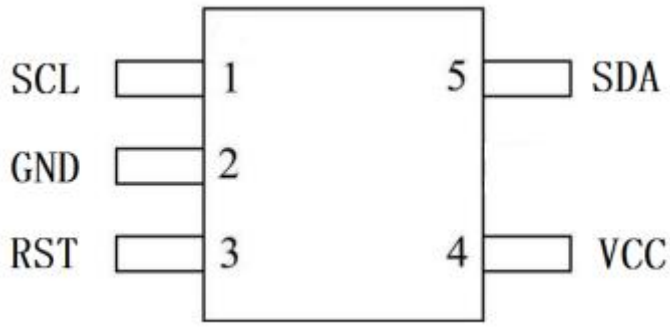


图1-2： LCS2110R SOT23-5 引脚说明

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		3.0~5.5	V
TA	工作温度		-40~85	℃
TSTG	存储温度		-45~105	℃

DC 特性：

符号	说明	条件	最小	典型	最大	单位
VCC	工作电压	3.3V 工作模式	3.0	3.3	3.6	V
		5V 工作模式	4.5	5.0	5.5	
ICC	工作电流	@内频 25MHz		4.0	5.0	mA
IPD	低功耗（关断模式）				0.1	uA

电特性：

符号	说明	单位	条件	VCC	Min	Max
VIL	Input Low Voltage	V		3.3V	2	5.5
				5V	0.7xVCC	5.5
VIH	Input High Voltage	V		3.3V	0	0.8
				5V	0	0.7xVCC
VHYS	Schmitt trigger hysteresis	V		3.3V	0.1xVCC	
				5V		
IIH	Input High Current	uA		3.3V	——	+1
				5V		

IIL	Input Low Current	uA		3.3V	-1	——
				5V		
VOL	Output Low Voltage	V	High driving: IOH=4.5mA Low driving: IOH=2.25mA	3.3V	——	0.4
			High driving: IOH=6mA Low driving: IOH=3mA	5V	——	0.5
VOH	Output High Voltage	V	High driving: IOH=4.5mA Low driving: IOH=2.25mA	3.3V	2.4	——
			High driving: IOH=6mA Low driving: IOH=3mA	5V	VCC-0.8	——
Rpup	Pull up resistor	KOhm		5V/3.3V	22	50
Rpdn	Pull down resistor	KOhm		5V/3.3V	20	100
CIN	I/O input Capacitance	pF		5V/3.3V	——	10

1.4 产品特性

1.4.1 调试资源

- 安全 CPU 内核，32 位通用 CPU
- 全球唯一硬件 ID 与管理编码
- 支持 IIC 通讯
- 16K 字节密钥文件存储区
- 支持 DES、3DES 算法
- 支持 AES128、AES192、AES256
- 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。

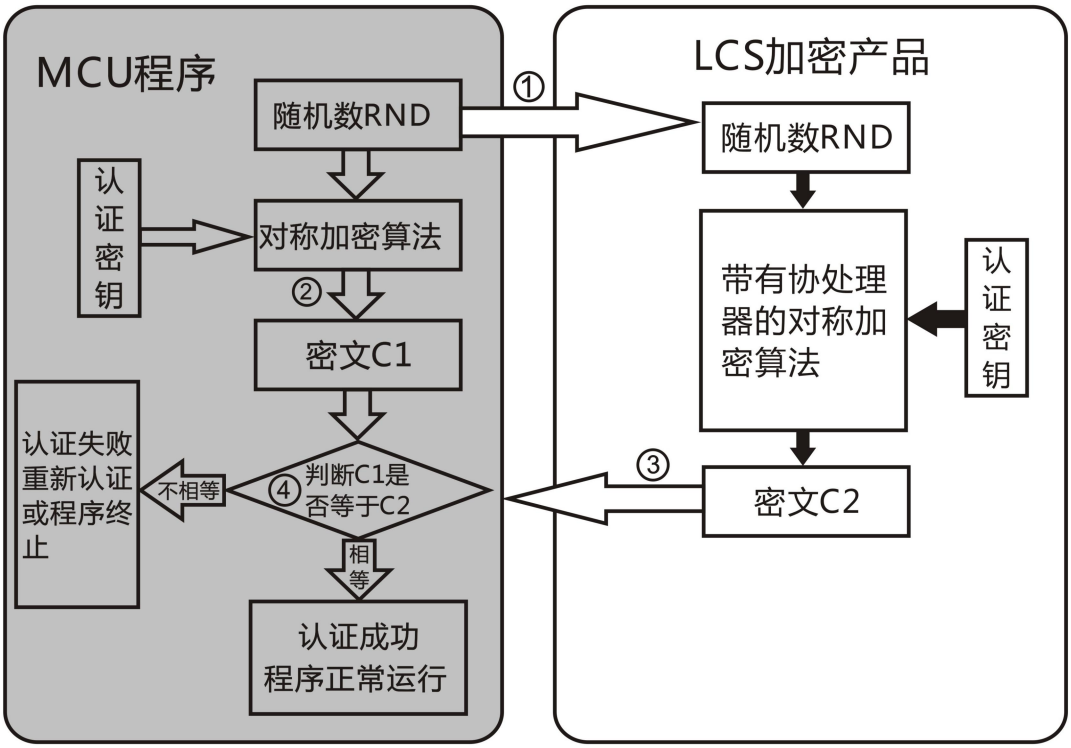


图 2-1： 安全认证方案概念

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

LCS2110R 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 LCS2110R 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 LCS2110R 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 LCS2110R 中，用户只需按照规定的 APDU 指令协议与 LCS2110R 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

LCS2110R 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。

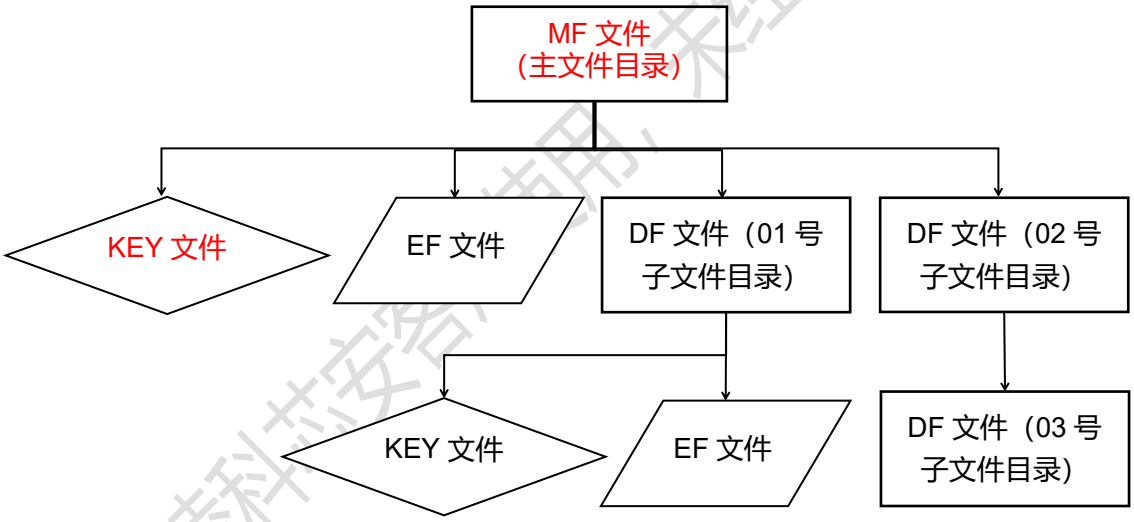


图 3-1： 基本文件结构

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。

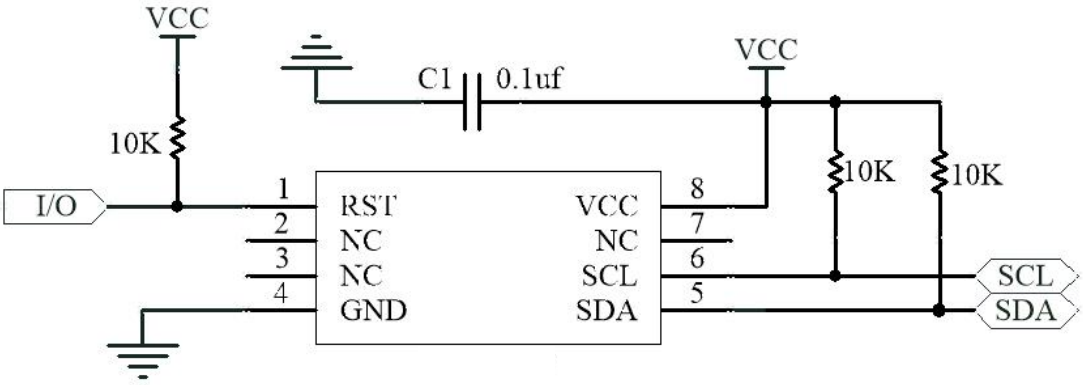
3.2.2 密钥更新使用权限

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。

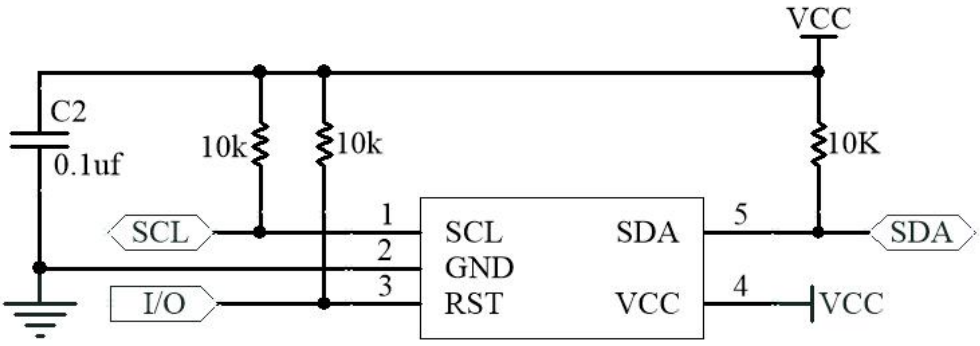
第 4 章 通讯调试说明

4.1 通讯电路

Sop8 封装：



Sot23-5 封装：



LCS2110-sot23

4.2 通讯时序

4.2.1 复位时序

电源正常供给后，当 LCS2110R 的 RST 引脚出现由低到高的时序后，LCS2110R 将执行复位操作，复位操作大概需要 10ms 完成。时序如图 4-1 所示。

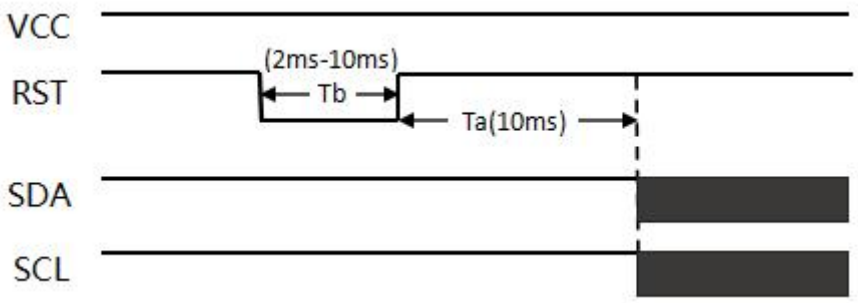
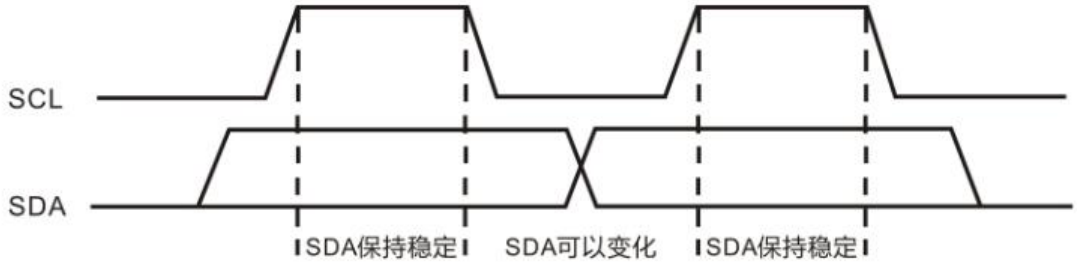


图 4-1： 复位时序

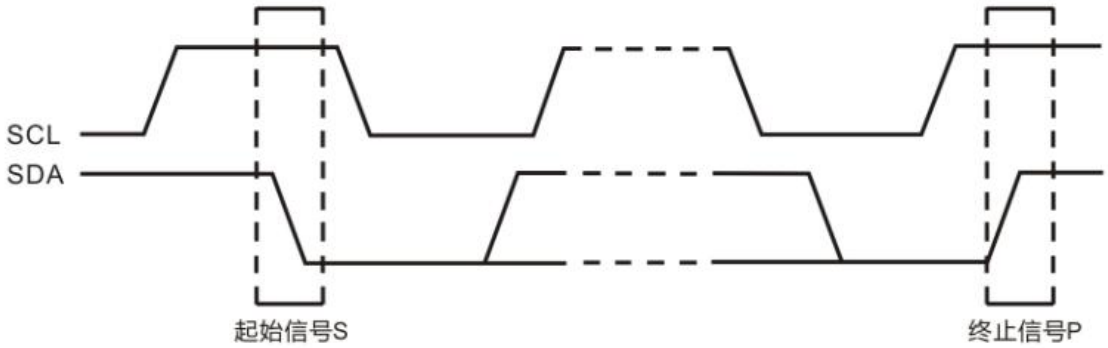
4.2.2 IIC 通讯时序

（1） 数据位的有效性规定



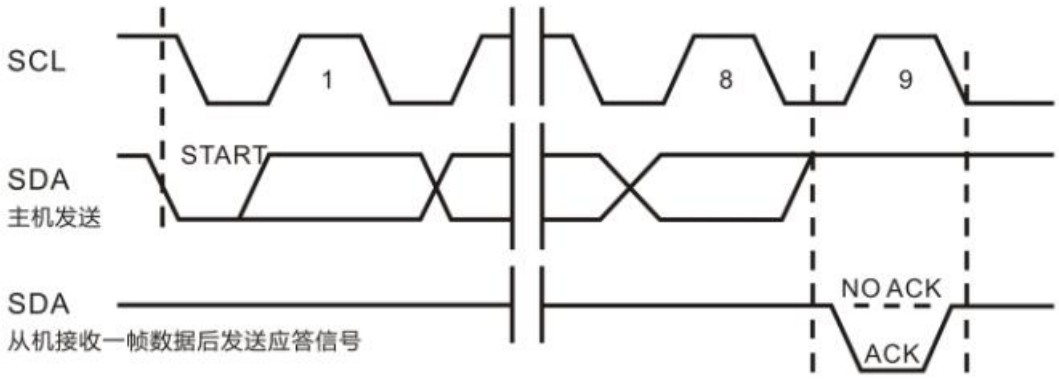
I2C 总线进行数据传送时，时钟信号为高电平期间，数据线上的数据必须保持稳定，只有在时钟线上的信号为低电平期间，数据线上的高电平或低电平状态才允许变化。

（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）。

4.3 指令协议

LCS2110R IIC 指令采用凌科芯安自定义指令协议格式。

注：文档中的参考指令全部为 16 进制数据。

LCS2110R 芯片 I2C 从器件地址为 0x50(8 位地址)

4.3.1 IIC 通讯协议指令格式

LCS2110R IIC 输入命令格式，如表 4-1 所示。

写指令	参数含义	长度（字节）
Add_W	写地址	1
Ld	后续指令长度	2
Cmd	命令内容	指令自身长度

表 4-1： 输入命令格式

LCS2110R IIC 输出命令格式，如表 4-2 所示。

读数据	参数含义	长度（字节）
Add_R	读地址	1
Ld	后续数据字节长度	2
Data	返回数据内容	Ld-2
Sw	状态码	2

表 4-2： 输出命令格式

4.3.2 指令测试

从 LCS2110R 中获取 8 字节随机数的指令和输出数据如表 4-3 和 4-4 所示。

写指令	内容	长度（字节）
Add_W	50	1
Ld	00 05	2
Cmd	00 84 00 00 08	5

*表 4-3：*获取 8 字节随机数的指令

输出数据如下表所示。

读数据	内容	长度（字节）
Add_R	51	1
Ld	00 0A	2
Data	8字节随机数	8
Sw	9000	2

*表 4-4：*接收到的数据

实际交互流程如图 4-2 所示。

注：“->”代表 MCU 向 LCS2110R 发送指令，“<-”代表 LCS2110R 向 MCU 返回响应数据。

图 4-2 为 MCU 与 LCS2110R 的完整交互流程。

```
->50 0005 0084000008                  //Add_W: 50 + Ld:0005 + Cmd: 0084000008

->51                                  //Add_R: 51

<- 000A 49CD44EB3724D437 9000         //Ld : 000A + Data: 49CD44EB3724D437
                                        (随机数) + Sw: 9000
```

*图 4-2：*获取随机数完整交互流程

4.4 关断模式设置

LCS2110R 芯片支持关断模式，可有效降低功耗。用户可选择主动或自动两种方式进入关断模式。主动方式发送指令后可立刻进入关断模式，被动方式设置好窗口时间后，当达到时间阈值自动进入关断模式。

4.4.1 主动进入关断模式

LCS2110R 接收到主机发送的指令后会立即进入关断模式，交互指令如表 4-5 所示。

写指令	内容	长度（字节）
Add_W	50	1
Ld	00 05	2
Cmd	00 00 00 00 00	5

表 4-5：主动进入关断模式

4.4.2 开启自动进入关断模式功能

LCS2110R 设置窗口时间后，若在窗口时间内 IIC 总线一直处于空闲状态，则 LCS2110R 会自动进入关断模式。设置窗口时间的指令如表 4-6 所示。该指令为芯片配置指令，应在正式应用前做好配置工作，禁止在产品正式应用过程中使用该指令！

写指令	内容	长度（字节）
Add_W	50	1
Ld	00 07	2
Cmd	80CC 0004 02 XXYY	7

表 4-6：设置窗口时间的指令

Cmd 中的 XX 表示 IIC 总线空闲 XX 秒后，自动进入关断模式，YY 是 XX 的取反结果。例如：MCU 发送 80CC 0004 02 05FA 指令后，加密芯片在总线空闲 5 秒后进入关断模式。

LCS2110R 输出响应数据如表 4-7 所示。

读数据	内容	长度（字节）
Add_R	51	1
Ld	00 02	2
Sw	9000	2

表 4-7：LCS2110R 响应状态数据

4.4.3 关闭自动进入关断模式功能

该指令为芯片配置指令，应在正式应用前做好配置工作，禁止在产品正式应用过程中使用该指令！

关闭指令和输出响应数据如表 4-8 所示。

写指令	内容	长度（字节）

Add_W	50	1
Ld	00 07	2
Cmd	80CC 0004 02 00FF	7

*表 4-8：*关闭自动进入关断模式的指令

LCS2110R 输出响应数据如表 4-9 所示。

读数据	内容	长度（字节）
Add_R	51	1
Ld	00 02	2
Sw	9000	2

*表 4-9：*接收到的数据

4.4.4 唤醒关断模式

当 LCS2110R 处于关断模式中，主机将 IIC 总线的 SDA 数据线拉低 1us 再拉高 5ms，即可唤醒芯片。唤醒时序如图 4-3 所示。

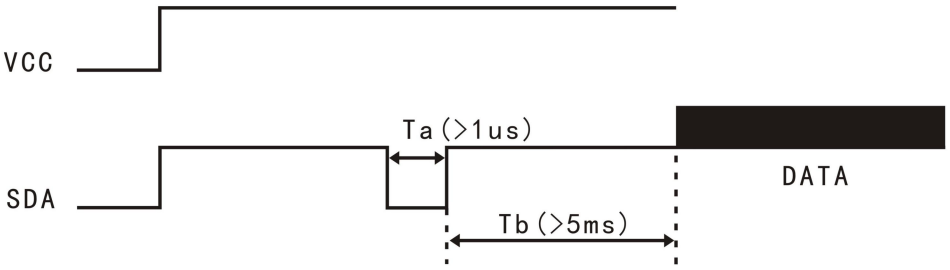


*图 4-3：*唤醒时序

注意：IIC_SDA 拉低 1us 以上即可，没有上限时间要求。

第 5 章 加密方案开发说明

5.1 安全认证方案开发流程

5.1.1 开发阶段准备工作

- MCU 端移植 3DES 算法，预置 3DES 认证密钥 KEY1，编写随机数生成函数。
- LCS2110R 建立基本文件结构，预置 3DES 认证密钥 KEY2，且 KEY2=KEY1。

  LCS2110R 建立基本测试文件结构的指令如下。

5.1.1.1 建立 MF 文件

-> 80E0 3F00 0D 38FFFFF0F0FFFFFFFFFFFFFFFF

<- 9000

5.1.1.2 建立 Key 文件

-> 80E0 0000 07 3F0050FFF0FFFF

<- 9000

5.1.1.3 写入 KEY2

-> 80D4 0100 15 30F0F00101 000000000000000000000000000000000

<- 9000

密钥 KEY2 长度 16 字节，由用户定义

5.1.2 应用阶段实现流程

应用阶段由 MCU 发起认证操作，先对 LCS2110R 进行复位操作，使其完成初始化操作。然后 MCU 自身生成随机数并发送给 LCS2110R，两端同时对随机数加密，并在 MCU 端对加密结果进行比较，结果相同认证成功，结果不同认证失败。具体流程详见图 5-1 所示。

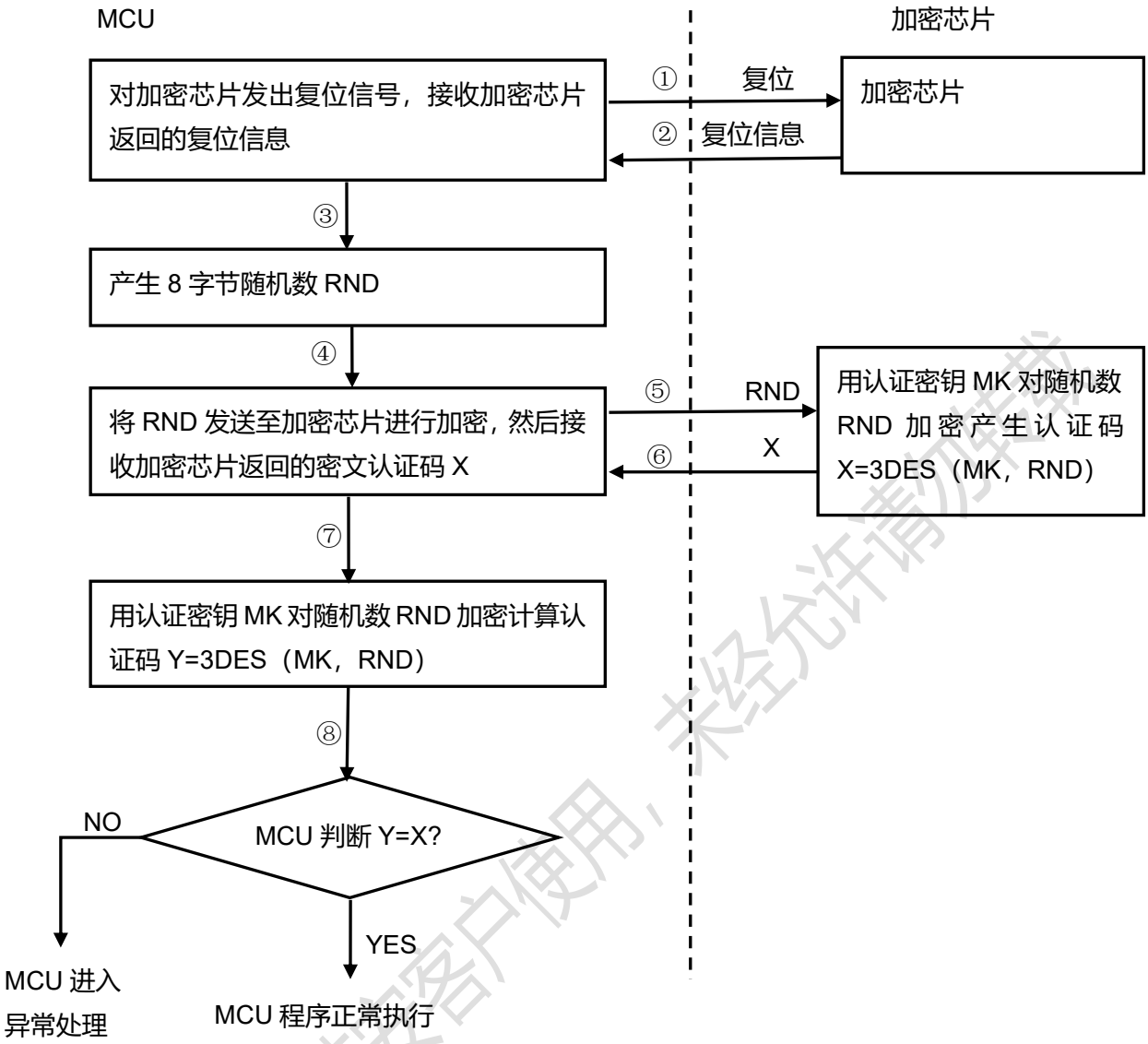


*图 5-1.*安全认证方案应用流程

5.1.3 调试注意事项

所有通讯数据均为 16 进制数据。

复位信息的最后 8 字节是芯片唯一 ID 号。

3DES 认证密钥 KEY1 和 KEY2 的长度为 16 字节，且 KEY1=KEY2。

随机数 RND 长度为 8 字节。

3DES 源码位于“LCS2110R 开发套件\通用加密算法源码”文件夹内。

5.1.4 3DES 算法源码函数接口说明

3DES 加密函数如表 5-1 所示。

表 5-1 : 3DES 加密函数

函数描述	说明
函数形式	Extern void encrypt_3des(uint8_t *inoutdata,uint8_t *keyStr);
参数 1	[IN OUT] 输入明文，输出密文
参数 2	[IN] 密钥

3DES 解密函数如表 5-2 所示。

表 5-2 : 3DES 解密函数

函数描述	说明
函数形式	extern void decrypt_3des(uint8_t *inoutdata ,uint8_t *keyStr);
参数 1	[IN OUT] 输入密文，输出明文
参数 2	[IN] 密钥

5.2 数据加解密方案开发流程

用户需要先建立应用文件结构才可以实现数据加解密功能。基本文件结构请参考第 3 章。建立结构时涉及到文件大小，读写权限，密钥使用权限等问题，用户可选择参考开发套件中的《LKCOS 智能操作系统参考手册 V3.3》自行设计测试脚本，也可由凌科芯安技术支持人员协助完成脚本设计。因为权限和密钥属性问题直接关系到核心安全且应用较为复杂，建议用户正式定版前，将应用结构提供给凌科芯安技术支持人员完成校核把关。

第 6 章 LCS KIT 软件使用

6.1 使用 LKT- K100 发行

6.1.1 连接开发板

LCS2110R 芯片放入 SOP8 的转接座（芯片的凹点或白点与图 6-1 中红圈对应）。将开发板与 PC 连接。

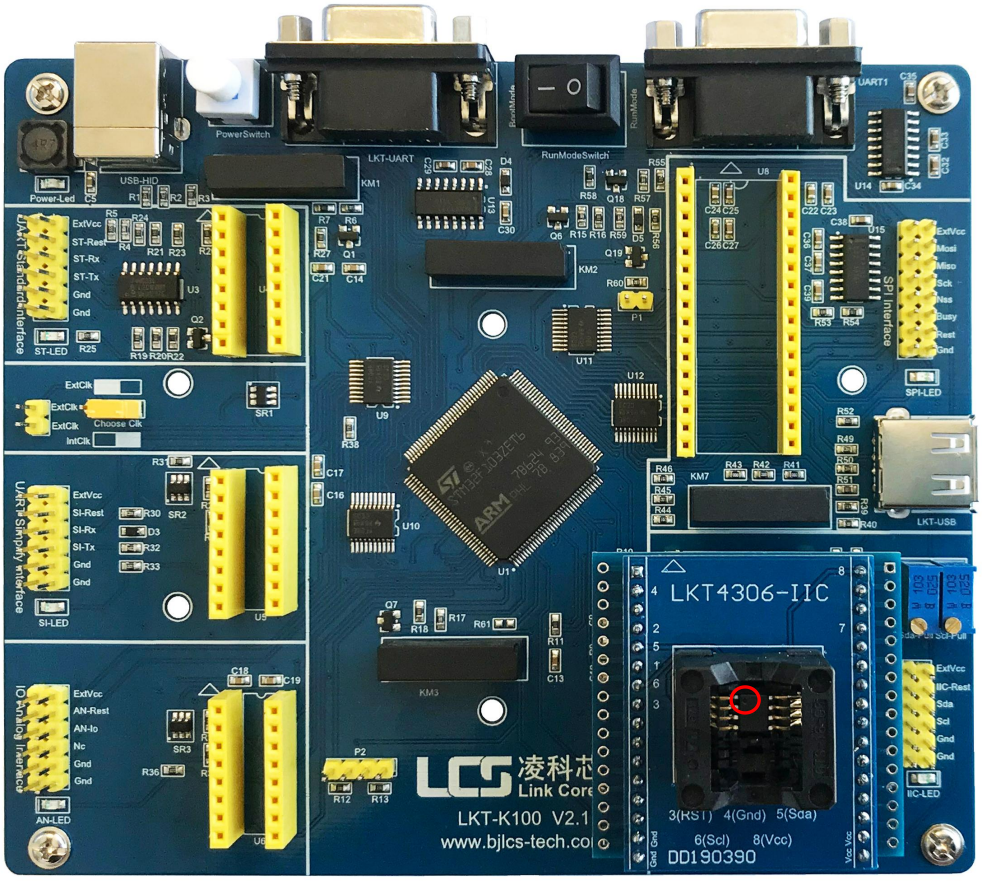


图 6-1：放入芯片

打开LCS KIT软件，如图6-2所示。

1. 在“通讯设置”页面下选择“通信方式”为“HID”，“协议属性”为“IIC”。
2. 点击“连接”，会弹出“HID 读写器”的对话框，如图 6-2 所示。
3. 点击“确定”按钮，会显示当前的连接状态，如图 6-3 所示。


LCS LCS KIT 4.0
通讯设置
COS指令
凌科芯安 Link Coresafe
通信方式
HID PCSC DLL
协议属性
UART
停止位 2 校验位 Even
Clk时钟 3579545 (Hz)
波特率 自动检测
IIC
器件地址 50 使用默认地址
SPI
通信操作
连接
断开
复位
清空显示
HID读写器
设备列表
LKT-K100 Smart Device (PID:4FF6)
刷新列表
确认
未连接
凌科芯安科技（北京）有限公司 http://www.bjlcs-tech.com

图6-2

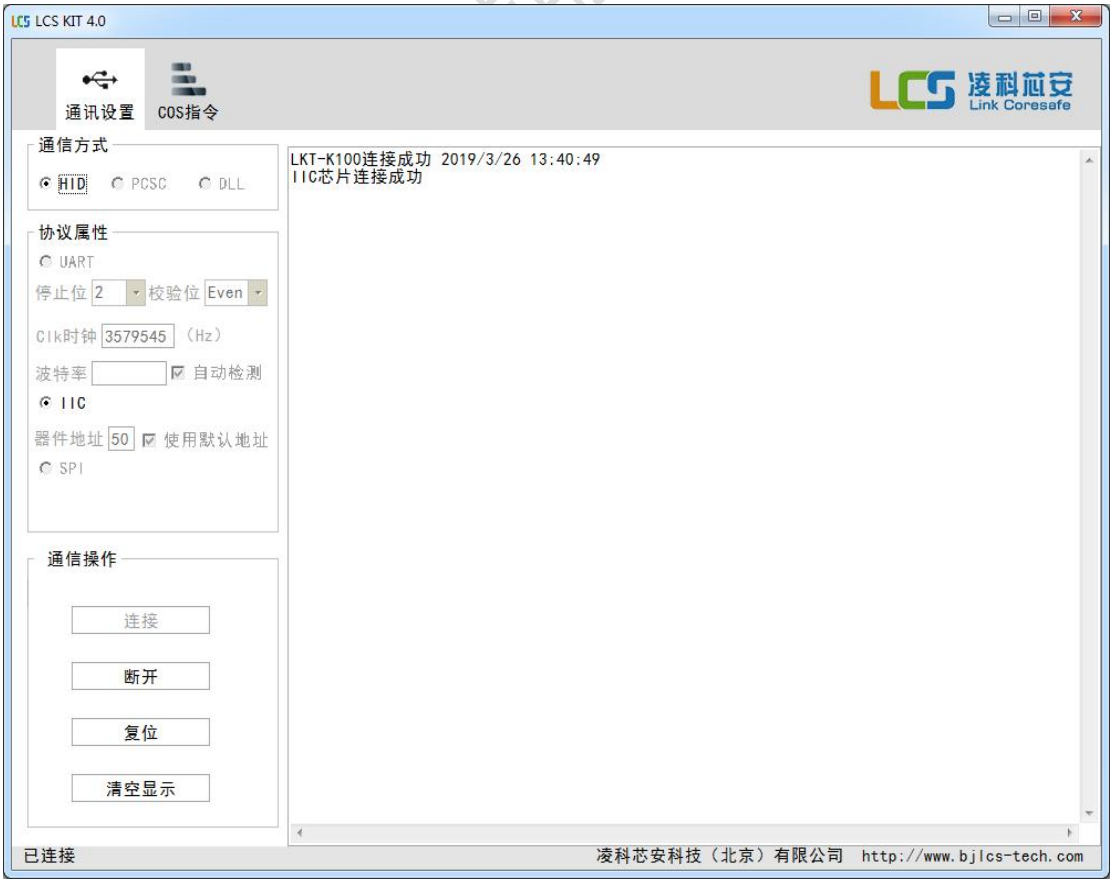

LCS LCS KIT 4.0
通讯设置
COS指令
凌科芯安 Link Coresafe
通信方式
HID PCSC DLL
协议属性
UART
停止位 2 校验位 Even
Clk时钟 3579545 (Hz)
波特率 自动检测
IIC
器件地址 50 使用默认地址
SPI
通信操作
连接
断开
复位
清空显示
LKT-K100连接成功 2019/3/26 13:40:49
IIC芯片连接成功
已连接
凌科芯安科技（北京）有限公司 http://www.bjlcs-tech.com

图 6-3

6.1.2 快速创建命令

点击“COS指令”进入指令操作界面，通过左侧的操作选项可以快速完成文件的创建、读写、选择以及密钥的增加修改等功能。由于LCS2110R出厂时已建立MF和默认KEY文件，通过COS选项选择MF主文件的方法如下，点击“选择文件”，在弹出的对话框中设置参数。如勾选“立即执行”，在生成指令后将自动执行该指令。否则生成指令后，不执行该指令，如图6-4所示。

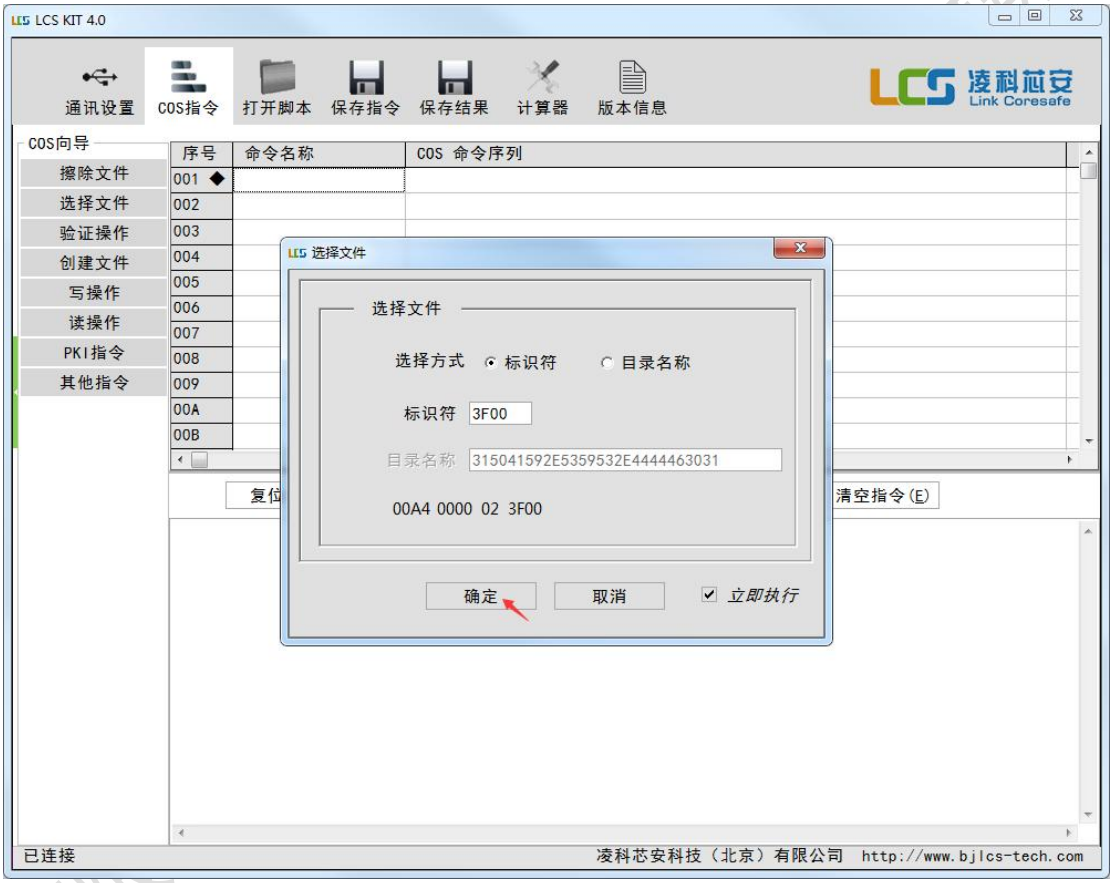


图 6-4：文件选择

6.1.3 自定义命令

如果开发人员对 LKCOS 指令比较熟悉，或操作不常见指令时，可自定义指令。选择“其他指令”->”自定义命令”如图 6-5 所示。

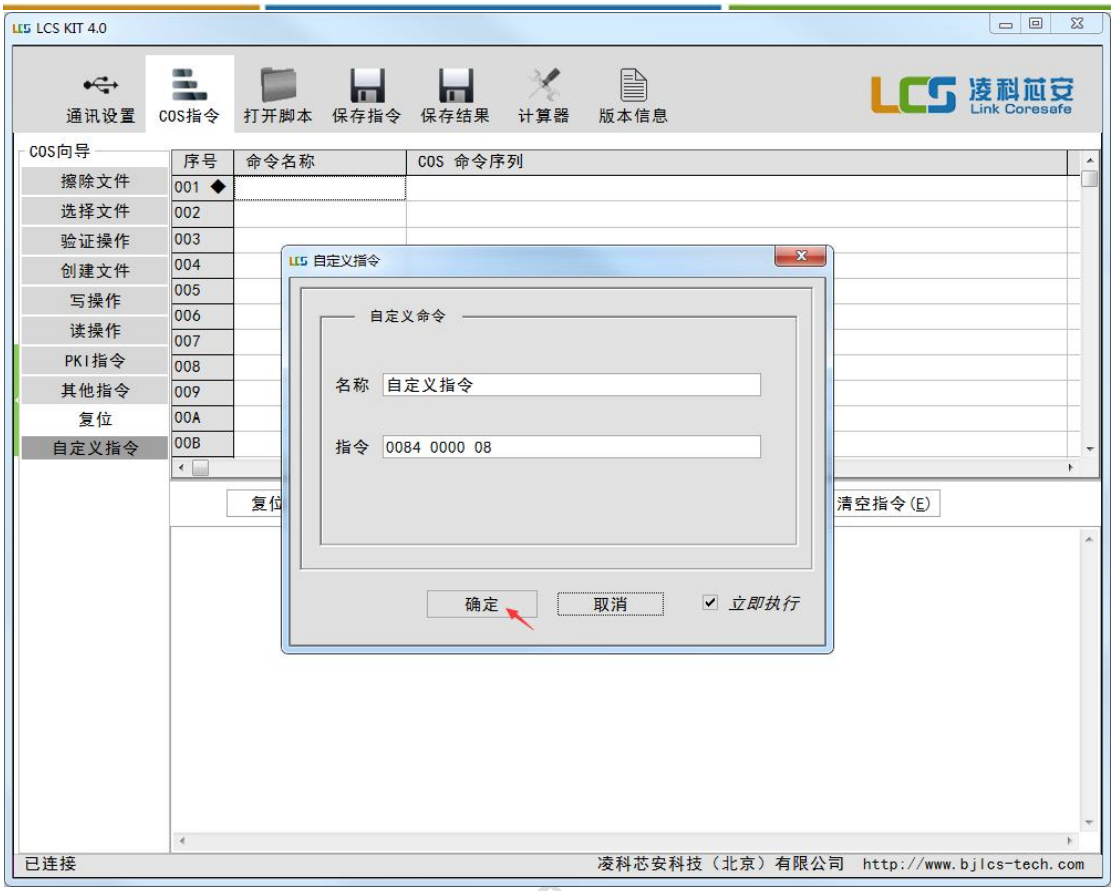


图 6-5：自定义命令演示

注：自定义命令并不是可由开发人员根据自己的想法任意定义。比如 LCS2110R 内部支持 MAC 算法，COS 向导没有快速创建 MAC 加密命令选项时，可在此处输入相应的命令，在指令区显示出所创建的命令名称和 APDU 指令，用于以后保存脚本实用。即“自定义命令”选项只能输入 LKCOS 的标准 APDU 指令。

6.1.4 脚本命令

如图 6-6 所示。点击“打开脚本”按钮，可以选择 COS 的脚本文件执行；点击“保存指令”按钮，可以将执行指令保存至指定文件中；点击“保存结果”按钮，可以将执行的结果保存至指定文件中。

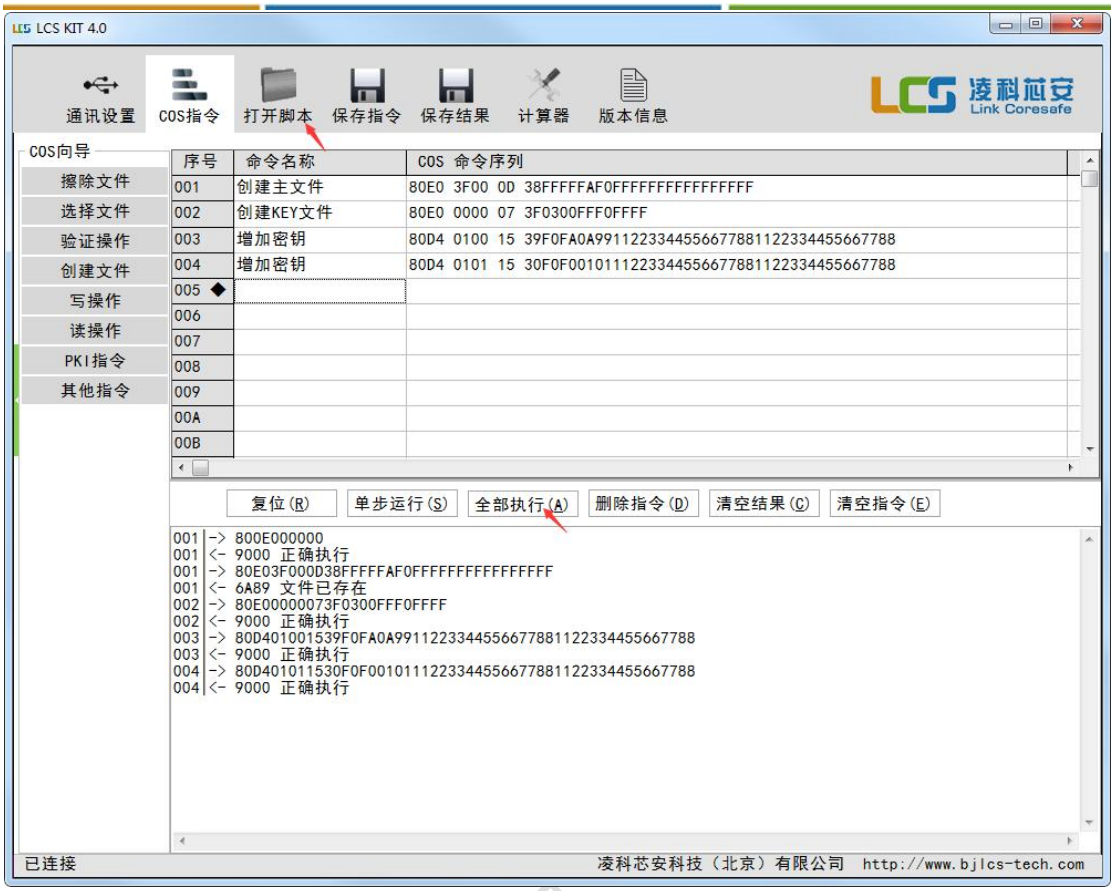


图 6-6： 脚本指令执行

6.1.5 辅助功能

LCS KIT 软件提供 DES/3DES、MAC 计算等辅助功能供开发使用。点击“计算工具”，如图 6-7 所示。

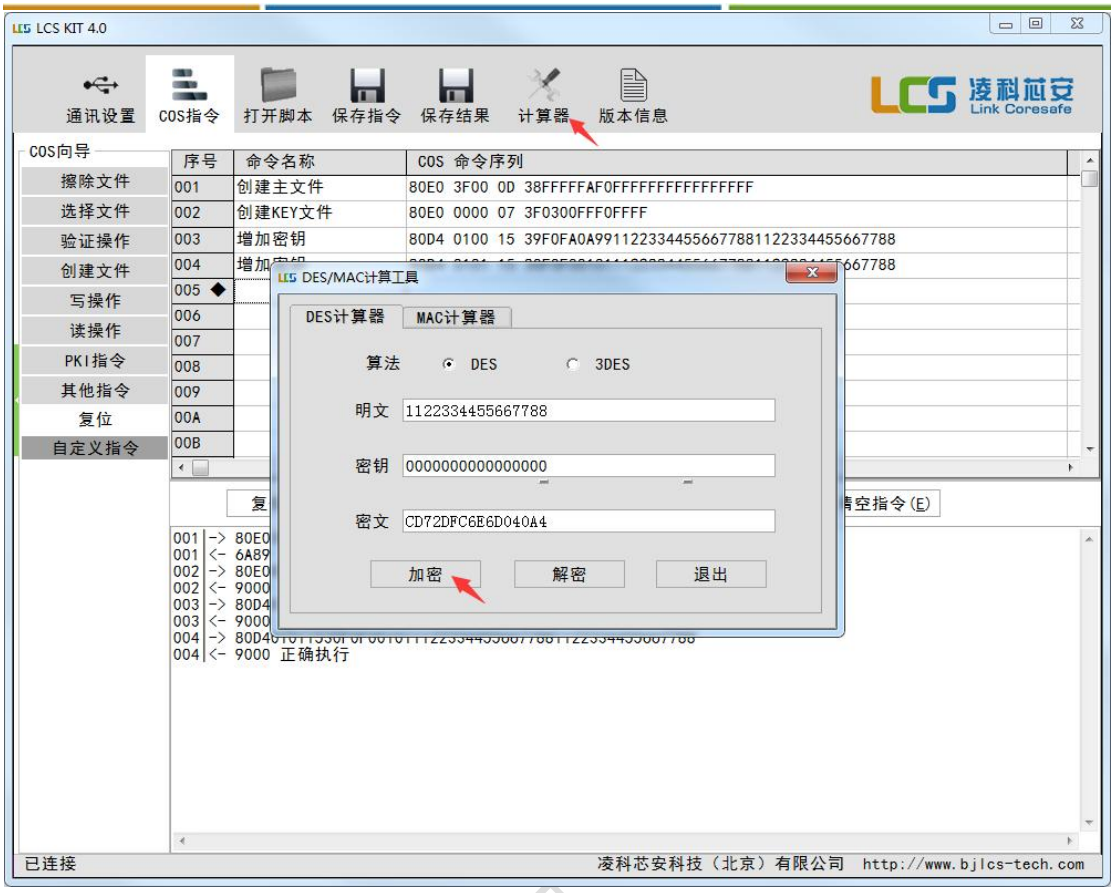


图 6-7： 计算工具

6.2 使用 P2000 烧录板发行

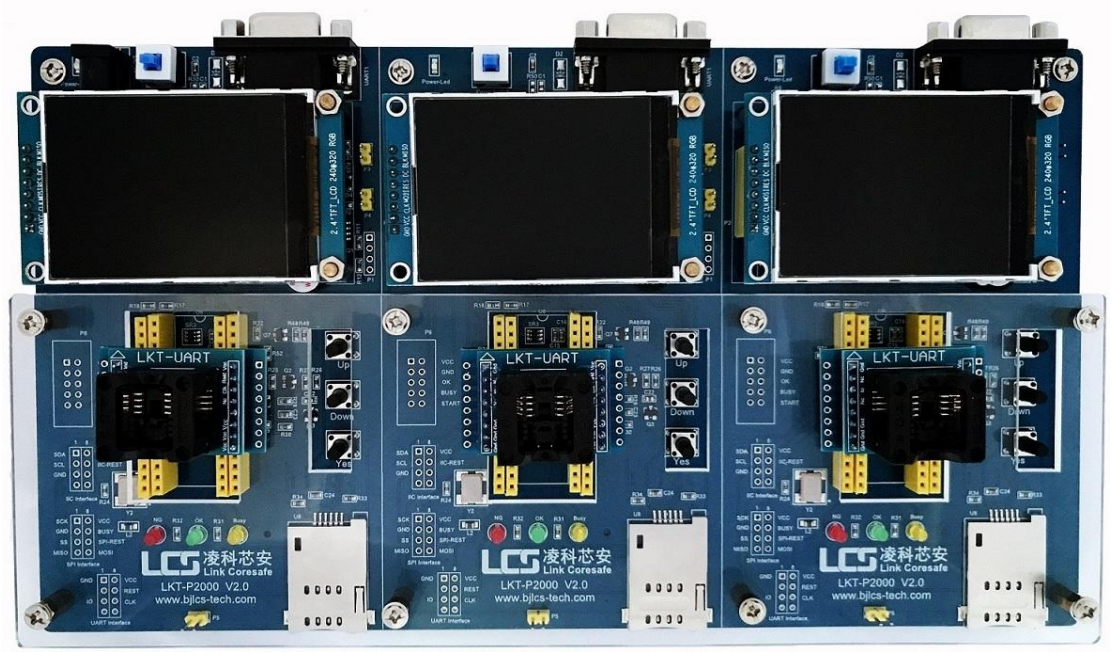


图 6-8 : P2000 下载器

P2000 烧录板可同时烧录 3 颗芯片，详情请联系技术支持。

第 7 章 芯片封装

LCS2110R 标准封装为 SOP8，如图 7-1 所示。也支持 SOT23-5 封装，如图 7-2 所示。也支持定制其他封装形式。

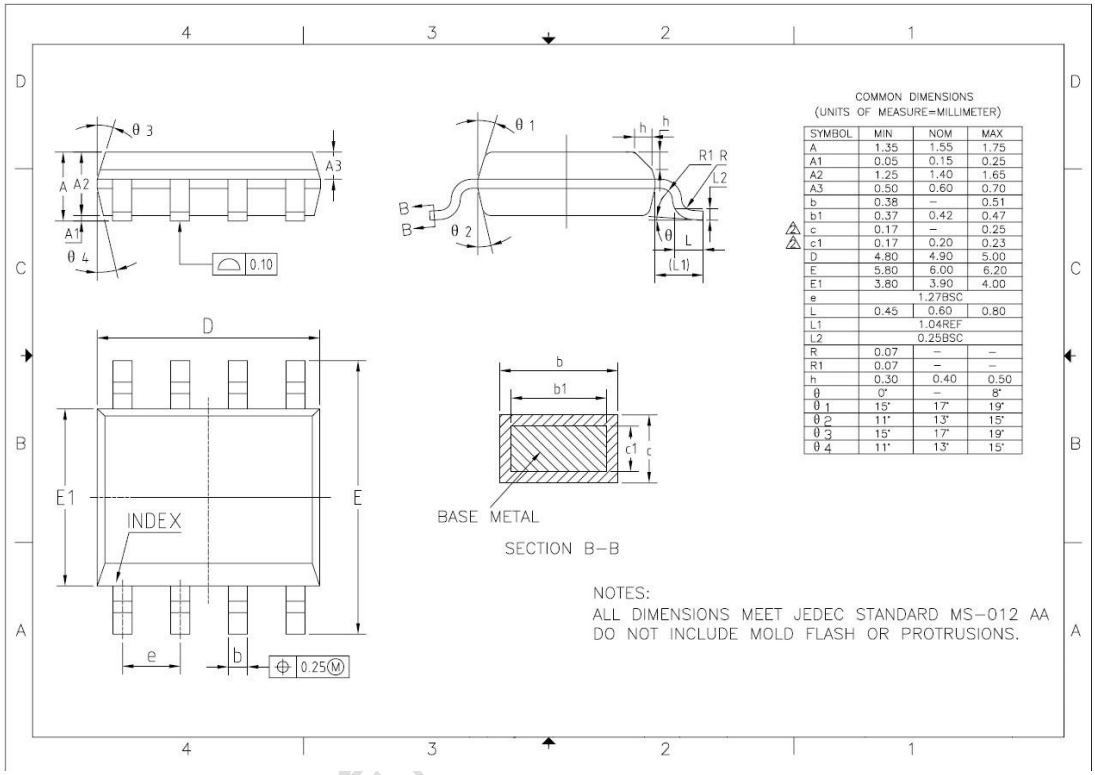
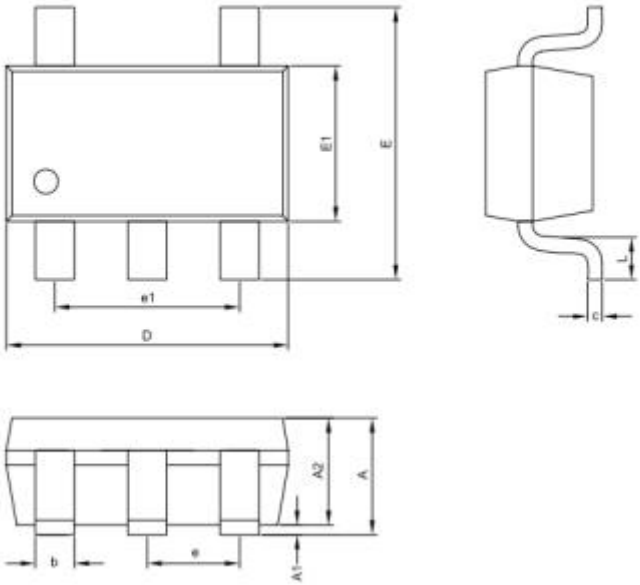


图 7-1： SOP8 封装图

SOT23-5



Symbol	Dimensions In Millimeters	
	Min	Max
A	1.050	1.250
A1	0.000	0.100
A2	1.050	1.150
b	0.300	0.500
c	0.100	0.200
D	2.820	3.020
E	2.650	2.950
E1	1.500	1.700
e	0.950typ	
el	1.8	2.000
L	0.300	0.600

图 7-2： SOT23-5 封装图