LKT4105 用户手册

凌科芯安科技（北京）有限公司

版本记录（内部）

当前版本		V4.1	2015.02
原始版本		V3.1	2014.03
升级说明			
升级日期	版本号	新增内容	修改内容
2015.02	V4.1		开发工具和上位机软件更新

版本记录（发给客户）

当前版本	V4.1	2015.02
升级说明		
升级日期	版本号	升级内容
2015.02	V4.1	开发工具和上位机软件更新

目　录

第 1 章 LKT4105 简介

1.1 概述

LKT4105 采用 EAL4+高安全等级，16 位智能卡芯片内核，芯片内部嵌入凌科芯安公司的 LKCOS 智能操作系统，用户可以把 MCU 中程序一部分关键算法函数移植到 LKT4105 芯片中运行。用户采用标准 C 语言编写代码，采用 16 位专用编译器编译 C 程序。在实际运行过程中，通过调用函数方式运行智能卡芯片内的程序段，并获得运行结果，并以此结果作为用户程序进一步运行的输入数据。LKT4105 成了产品的一部分，而算法在 LKT4105 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 LKT4105 中，当需要用到 LKT4105 中的算法时，MCU 向 LKT4105 发送指令，LKT4105 根据指令，在内部运行，返回结果给 MCU 如图 1-1 所示。

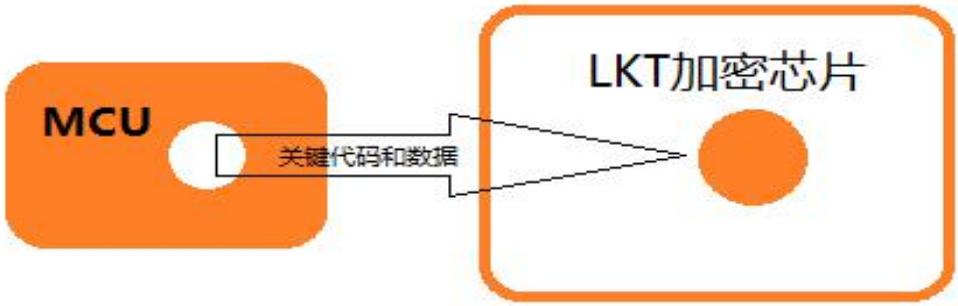

*图 1-1：*加密原理

1.2 LKT4105 产品特性

- 以最高安全等级的智能卡(EAL4+)芯片技术为基础，具有极高的软硬件安全性
- 实现算法下载，用户可灵活实现自有知识产权的保护
- 业内领先的16位加密操作系统技术，保证数据的安全性
- 标准DIP8或SOP8封装形式，另外还可为用户定制其他封装形式

1.2.1 硬件特性

- 采用16位智能卡芯片内核，内置16位加密操作系统
- 全球唯一硬件ID与管理编码
- 具有兼容uart串口
- 支持ISO7816 T=0和自定义A3通讯协议
- 具有32K字节超大用户程序下载空间（可以为客户定制容量）
- 4K字节可定义安全性NVM数据存储区
- 编译环境具有丰富的系统调用和开发接口

1.2.2 系统软件特性

- 自主知识产权的COS系统--LKCOS
- 片上操作系统(COS)进行通信、文件、存储、安全管理
- LKCOS提供16级安全控制等级
- 支持用户程序下载
- 支持用户自己定义参数的输入，输出

1.2.3 安全特性

(1) 硬件防护措施

- 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（读者 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
- 噪音的产生（对边信道攻击）
- 预硅功率分析

(2) 软件 - 操作系统防护措施

- 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
- 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

1.3 应用领域

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。

第 2 章 LKT4105 开发流程

CPU 的源代码应被分成两部分 ,分别存储到 CPU 和 LKT4105 内部。当程序运行时 CPU 通过发送算法命令调用 LKT4105 的算法。开发流程分为 6 个步骤如图 2-1 所示。

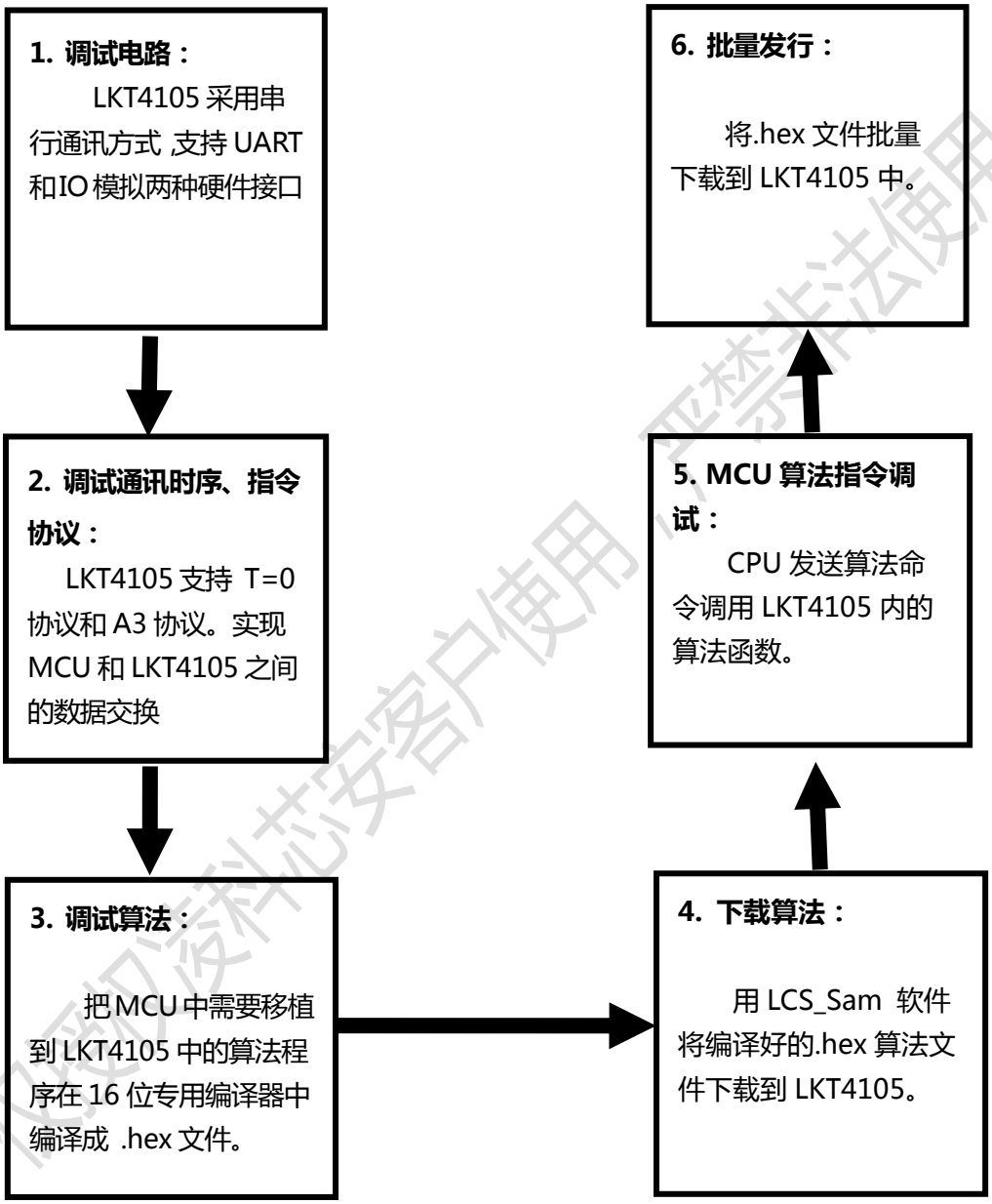

图 2-1：开发流程

第 3 章 通讯协议说明

3.1 指令协议

LKT4105 支持两种协议：T=0 协议和 A3 协议。区别在于命令头、命令格式不同，与向 LKT4105 内部算法传输的输入输出参数，和用户下载的算法没有关系。

- T=0 协议命令头是“8008 0000”,用户在 PC 上用 LCS_Sam 软件调试算法时，同时支持 T=0 和 A3 协议。
- A3 协议命令头是“A3”，用 MCU 调试算法时，同时支持 T=0 和 A3 协议。

注：命令全部是 16 进制

3.2 ISO7816 T=0 协议说明

T=0 协议基于智能卡 7816 标准，该协议交互流程复杂。

3.2.1 缩略语

APDU	应用协议数据单元
ATR	复位应答
CLA	类字节
CLK	时钟信号
GND	地 ，基准电压。
INS	指令字节
I/O	串行数据的输入/输出
Lc	在指令中发送的字节长度
Le	接收响应数据的字节长度
P1	参数1
P2	参数2
SW1	状态字节1
SW2	状态字节2
VCC	电源输入

表 3-1 : 缩略语

3.2.2 指令格式

命令由命令头和命令体两部分构成，如表3-2所示：

命令头				命令体		
CLA	INS	P1	P2	Lc	DATA	Le

*表 3-2：*指令结构

常见的指令构成形式，如表3-3所示：

形式	指令类型
CASE 1	CLA INS P1 P2
CASE 2	CLA INS P1 P2 Le
CASE3	CLA INS P1 P2 Lc Data
CASE 4	CLA INS P1 P2 Lc Data Le

*表 3-3：*指令类型

LKT4105 常用指令，如表3-4所示：

命令头				命令体			描述
CLA	INS	P1	P2	Lc	DATA	Le	
00	84	00	00	无	无	01-10	取随机数
80	08	00	00	XX	XX....XX	无	算法调用指令
00	C0	00	00	无	无	XX	取响应数

*表3-4：*常用指令

返回状态码的具体意义，如表3-5所示：

SW1	SW2	意义
90	00	正确执行
61	XX	有 XX 字节数据返回
67	00	长度错误
69	85	使用条件不满足
6A	86	参数 P1，P2 错误
6D	00	命令不存在
6E	00	无效的 CLA
6F	00	数据无效

*表 3-5：*SW

3.2.3 算法调用指令举例说明

使用 LCS_Sam 软件和用 CPU 测试 T= 0 协议的命令过程略有差别。 LCS_Sam 软件调用的是私有接口函数，接口函数对 INS 内部已经做了处理。在测试之前 LKT4105 必须下载算法。现在以“LKT4105 算法\ AppDemo”中的“fun_1”函数为例子。

使用 LCS_Sam 向 LKT4105 发送调用算法命令的流程如图 3-1 所示。

```
-> 80080000 09 01 0102030405060708   /**发送调用算法命令**/
<- 6108                              /**有 8 字节应答数据等待读出**/
-> 00C0000008                        /**发送获取数据命令**/
<< FEFDFCFBFAF9F8F79000              /**取出返回的数据以及 SW 值**/
```

*图 3-1：*LCS_Sam 执行过程

使用 CPU 向 LKT4105 发送调用算法命令的流程如图 3-2 所示。

```
-> 80080000 09                       /**发送命令头+LC**/
<- 08                                /**返回过程字节 INS**/
-> 01 0102030405060708               /**发送后续数据**/
<- 6108                              /**有 8 字节应答数据等待读出**/
-> 00C0000008                        /**发送获取数据命令**/
<- C0 FEFDFCFBFAF9F8F79000           /**取出数据（INS+算法返回数据 +SW）**/
```

*图 3-2：*CPU 执行过程

指令结构说明如表 3-6 所示。

命令头	LC	算法函数序号	传入算法函数中的参数
8008 0000	09	01	0102030405060708

*表 3-6：*算法指令结构说明

3.2.4 提速指令说明

当 LKT4105 芯片复位应答完全返回后，如果不发送任何调整 PPS（通讯速率）的命令，缺省通信速率为 bps = CLK/372，1etu = 372/CLK (其中 CLK 是提供给 LKT4105 的时钟频

率)。

如果给 LKT4105 的时钟频率 CLK = 3.579MHZ。则默认通讯速率 = 3579000Hz / 372 ≈ 9600bps。1etu = 372/3.579(M)≈104μs

提速指令与修改后的 PPS 值如表 3-7 所示。

提速指令	PPS 值
FF10947B	64
FF10957A	32
FF109679	16

*表 3-7：*PPS 值

LCS_Sam 软件调用是凌科芯安公司提供的接口函数，所以当使用 LCS_Sam 软件对 LKT4105 复位后，芯片默认分频系数为 372，发送提速指令后，开发板会根据芯片的复位信息自动修改分频系数，提高通讯速度，复位后生效。

1. 在测试指令中输入 “FFFC 0001 00”，点击“单步运行”，复位后提速指令生效。

2. 在测试指令中输入 “FFFC 0000 00”，点击“单步运行”，复位后恢复默认速度。

使用 LCS_Sam 对 LKT4105 提速的流程如图 3-3 所示。

```
-> FFFC000100                                  /****发送提速指令****/
<- 9000 正确执行
<- 3B7D940000420191680320121217008 2B95A       /****复位后提速生效****/
当前波特率 55921
-> FFFC000000                                  /****发送恢复默认速度指令****/
<- 9000 正确执行
<- 3B7D940000420191680320121217008 2B95A       /****复位后恢复默认速度****/
当前波特率 9630
```

*图 3-3：*修改 PPS

3.3 A3 协议说明

A3 协议是我司自定义的一种指令格式协议，其特点是交互流程简单。

3.3.1 指令格式

命令由命令头和命令体两部分构成如表3-8所示。

命令头	命令体	
A3	Lc	DATA

*表 3-8：*A3 指令结构说明

3.3.2 算法调用指令举例说明

在测试之前 LKT4105 下载好算法。现在以“LKT4105 算法\ AppDemo”中的“fun_1”函数为例子。

使用 CPU 或 LCS_Sam 软件向 LKT4105 发送调用算法命令的流程如图 3-4 所示。

```
-> A3 09 01 0102030405060708          /**发送调用算法命令**/
<- A3 0A FEFDFCFBFAF9F8F7 90 00   /**返回 A3 + 后续数据长度 + 算法返回数据内容 + 状态码（SW）
```

*图 3-4：*算法命令操作流程

指令结构说明如表 3-9 所示。

命令头	LC	算法函数序号	传入算法函数中的参数
A3	09	01	0102030405060708

*表 3-9：*算法指令结构说明

返回数据结构如表 3-10 所示。

命令头	后续数据长度	算法返回的数据	状态码（SW）
A3	0A	FEFDFCFBFAF9F8F7	9000

*表 3-10：*返回数据结构

第 4 章 LCS_Sam 软件使用

4.1 连接开发板

LKT4105 芯片放入 SOP8 的转接座（芯片的凹点或白点与图 4-1 中红圈对应）。将开发板与 PC 连接。

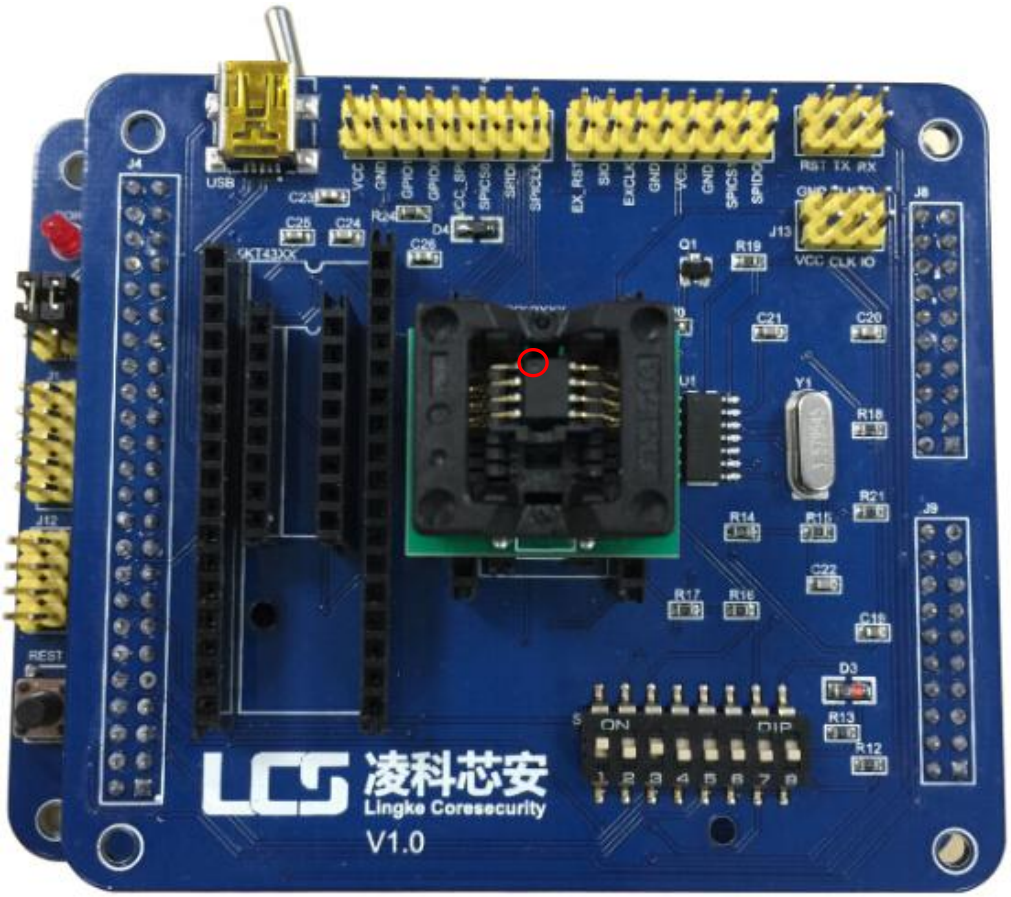

图 4-1 放入芯片

打开 LCS_Sam 软件，如图 4-2 所示。

1. 点击”设备通信“选项页，选择“HID”通信方式（默认）。
2. 在通信时钟输入框内，输入提供加密芯片的时钟频率（范围：1~5Mhz，默认 3.579MHz）。
3. 点击”连接“按钮，会显示当前的连接状态、时钟频率和波特率。

*图 4-2：*连接开发板

4.2 下载算法

1．点击”算法下载“选项页。

2．在”旧口令“中填写下载口令，默认下载口令为”0000000000000000“（口令长度必须为 8 字节)。

3．点击”打开文件“按钮，选择下载到加密芯片中的.hex 文件。

4．点击“算法下载”按钮下载算法，如图 4-3 所示。

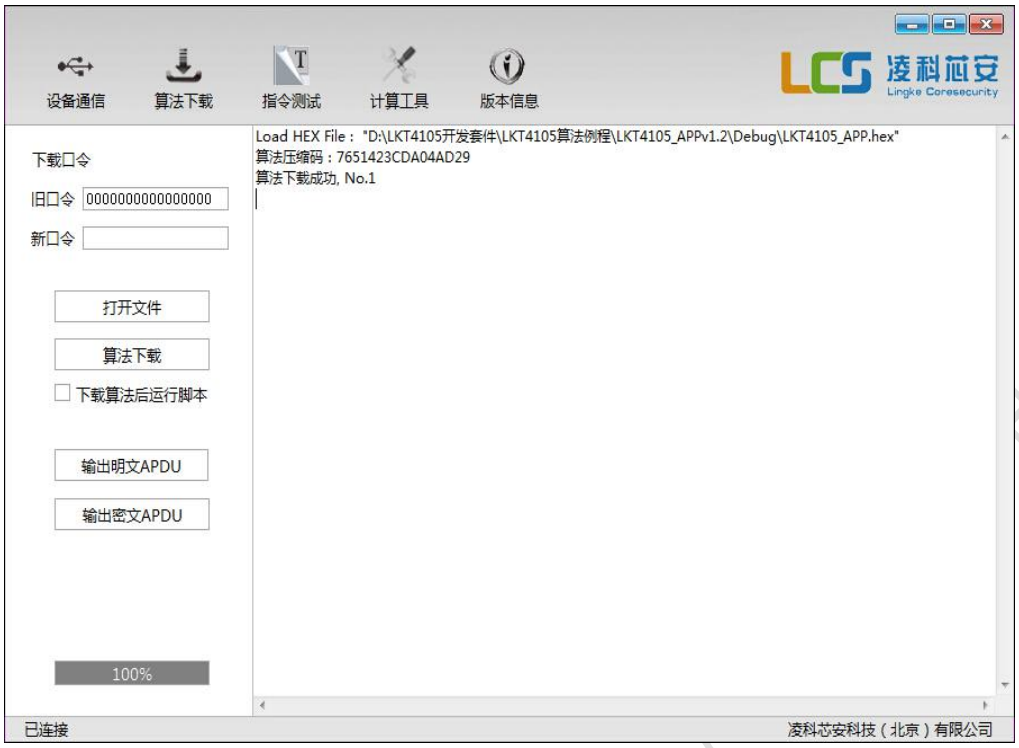

*图 4-3：*下载算法

4.3 修改下载保护口令

1. 在”算法下载“选项页中的”旧口令“输入框内，填入当前使用的下载口令，在”新口令“中，填入修改后的下载口令(口令长度必须为8字节)。

2. 点击“算法下载”，算法下载成功后完成修改。

修改下载口令后，该芯片只能用新口令下载算法，新口令与其它芯片无关（其他芯片默认口令仍为0000000000000000)。

4.4 发送算法指令

- 点击”指令测试“选项页。
- 在”测试指令“中输入算法指令。
- 点击”单步运行“，如图 4-4 所示。

图 4-4：发送指令

4.5 批量测试算法指令

批量测试例程中的几个算法指令步骤如下：

- 在”指令测试“选项页中，点击”打开脚本 “，选择脚本文件。
- 点击”批量运行“按钮，如图 4-5 所示。

*图 4-5：*运行脚本

第 5 章 算法移植介绍

LKT4105采用16位RISC内核（EAL4+）高端智能卡芯片平台，内置LKCOS智能操作系统。采用专用16位编译器编译程序。

移植算法函数时请直接打开我们提供的例程工程 LKT4105_App 这个工程直接编写和调试算法程序。例程里有详细注释，请按照注释要求编写算法程序。

*图 5-1：*LKT4105_App 工程文件

打开“App_Main.c”文件。

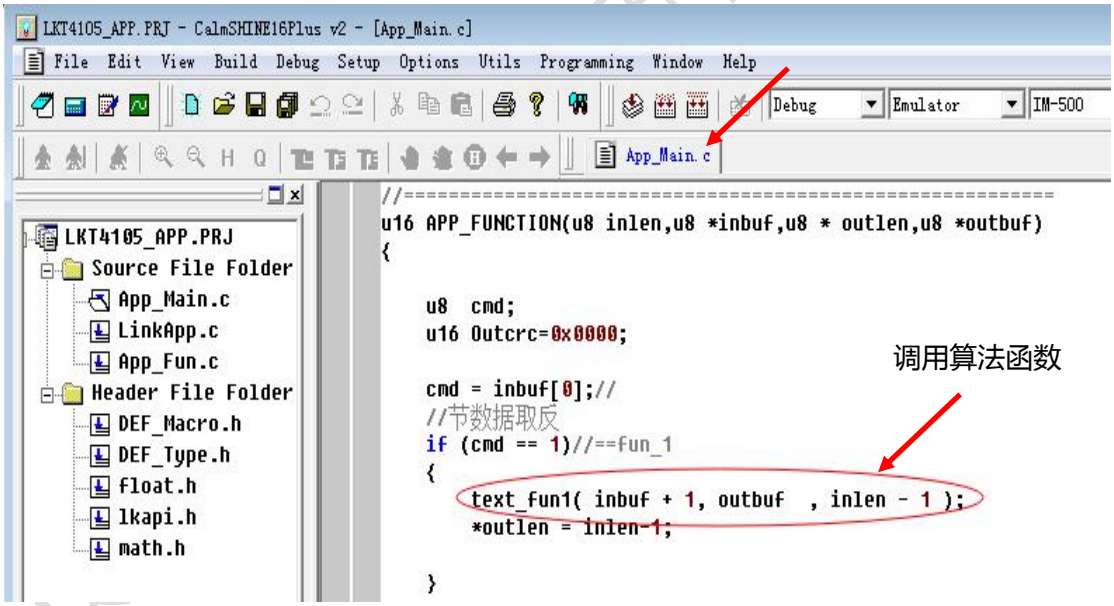

*图 5-2：*移植算法函数

附录 A：系统函数说明

LKT4105 提供 4K 字节的 NVM 数据存储区， 从地址“0x0000”到 “0x0FFF“。写 NVM 区函数如表 A-1 所示。

函数描述	说明
函数形式	extern void LK_WriteNvm(u16 addr， u8 *buf， u8 len);
参数 1	NVM 区地址
参数 2	写入的数据
参数 3	写入数据的长度

表 A-1： 写 NVM 区

读 NVM 区函数如表 A-2 所示。

函数描述	说明
函数形式	extern void LK_ReadNvm (u16 addr， u8 *buf， u8 len);
参数 1	NVM 区地址
参数 2	存放读出的数据
参数 3	读出数据的长度

表 A-2： 读 NVM 区

DES/3DES 加密函数。注意这三个参数都是 LV 结构(数据长度+数据 ，如加密数据时 08（长度） 1122334455667788(数据内容)）如表 A-3 所示。

函数描述	说明
函数形式	extern void LK_DESEncrypt(u8 *plain， u8 *k， u8 *cipher);
参数 1	明文长度+明文内容
参数 2	密钥长度+密钥值
参数 3	输出的密文长度+密文值

表 A-3： DES/3DES 加密

DES/3DES 解密函数。注意这三个参数都是 LV 结构(数据长度+数据 ，如解密数据时

08（长度） 1122334455667788(数据内容)）如表 A-4 所示。

函数描述	说明
函数形式	extern void LK_DESDecrypt(u8 *plain， u8 *k， u8 *cipher);
参数 1	需解密的密文长度+密文值
参数 2	密钥长度+密钥值
参数 3	解密后的明文长度+明文值

*表 A-4：*DES/3DES 解密

获取随机数函数见表 A-5。

函数描述	说明
函数形式	extern void LK_GetRandom(u8 *buf， u8 len);
参数1	存放随机数据
参数 2	获取随机数的位数

*表 A-5：*获取随机数

获取芯片 ID 号函数见表 A-6。

函数描述	说明
函数形式	extern void LK_GetChipID(u8 *sn);
参数1	存放芯片 ID 号

*表 A-6：*获取芯片 ID 号

附录 B：批量生产工具

凌科芯安科技（北京）有限公司 提供三款批量生产工具。

使用 LKT-K100 开发板下载算法如图 B-1 所示。

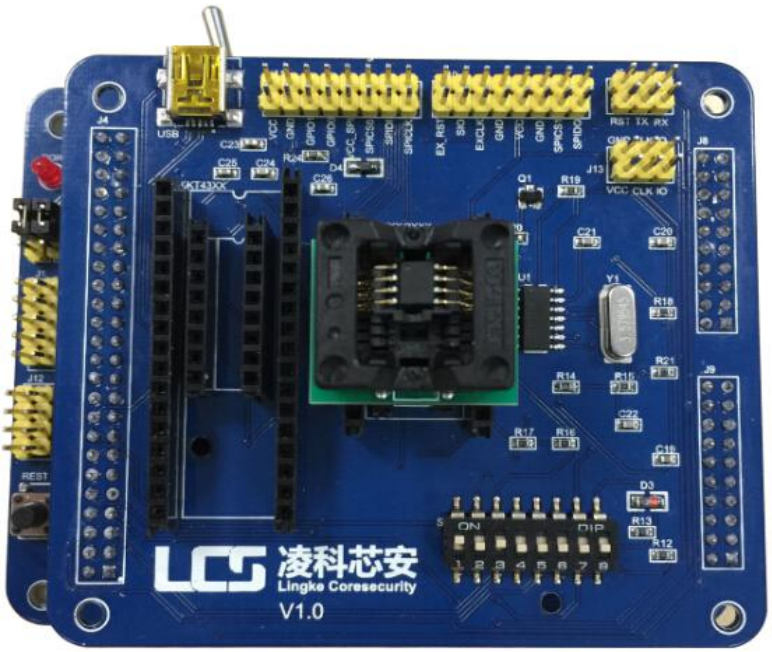

*图 B-1 :*LKT-K100 开发板

脱机烧写器批量下载算法如图 B-2 所示。

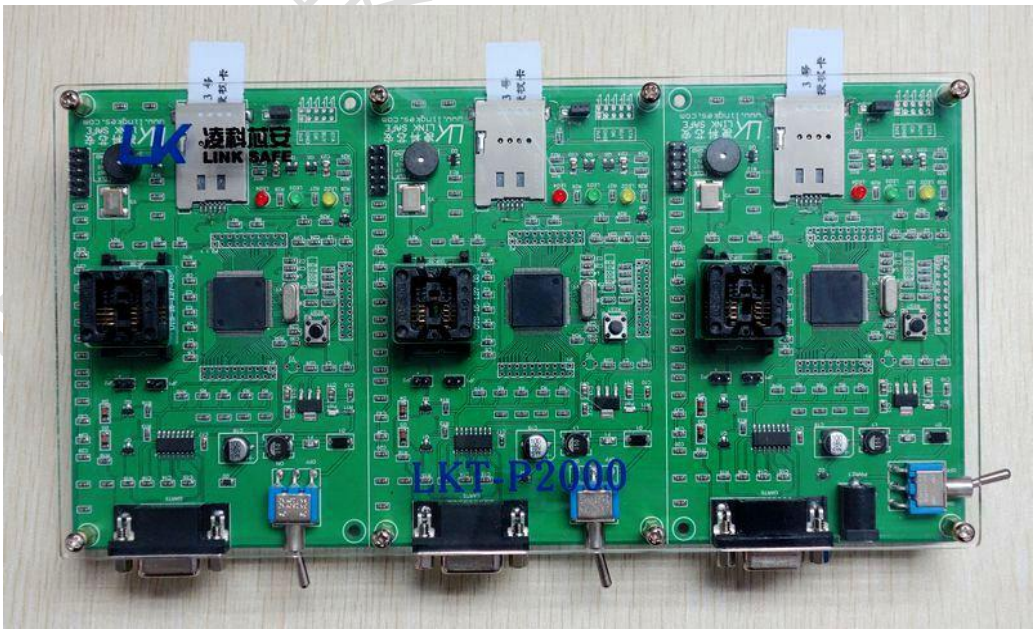

图 B-2 : P2000 下载器

自动机械手烧录，烧录器和机械手相连后，通过自动机械手自动烧录。见图 B-3。

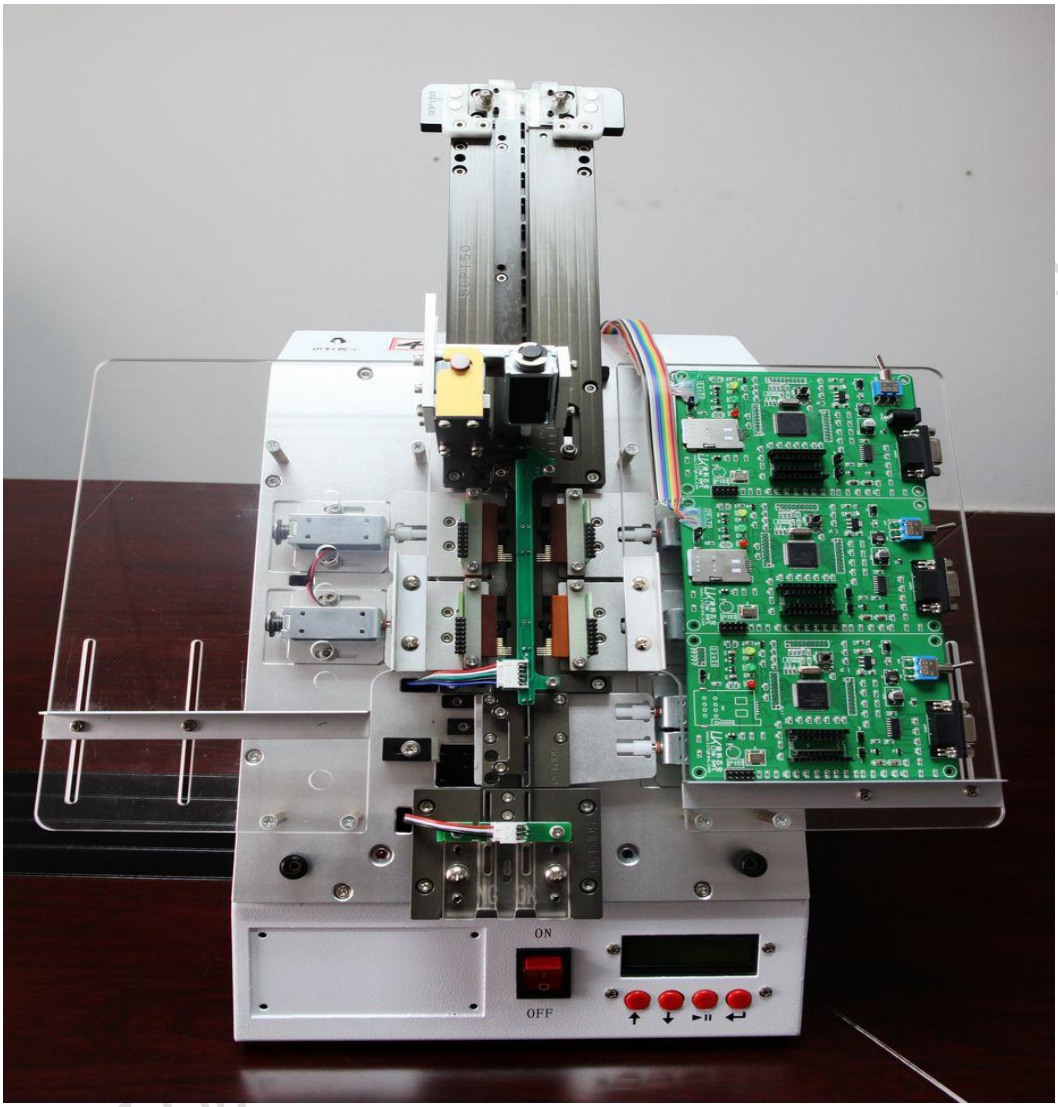

*图 B-3：*机械手