

密级状态：绝密（ ） 秘密（ ） 内部资料（ ☒ ） 公开（ ）

Mst6A628 高安芯片解密烧录指导

文件状态： [] 草稿 [] 正在修改 [<input checked="" type="checkbox"/>] 正式发布	文件标识	Mst6A628 高安芯片解密烧录指导
	文件编号	
	主要内容	
	当前版本	V1.0.0
	作 者	钟 斌
	完成日期	2016-3-30
	审 核	
	审核日期	

历史版本

时间	版本	内容	作者	备注
2016-3-30	V1.0.0	初版	钟斌	

TOP-TECH

目录

一、	说明	4
二、	解密及烧录方法	4
1、	停串口	4
2、	添加写 product key.....	4
1)	设置电脑时间	4
2)	解密 mstar debug 工具.....	4
3、	读取 Device ID.....	5
4、	解密	5
5、	通过 ISP 工具烧录 MBOOT	6

一、说明

对于加密的芯片在没有进行解密的情况下是无法通过 ISP 工具烧录 MBOOT、无法通过 DEBUG 工具读写寄存器，所以在碰到加密芯片时，得通过如下的方法进行解密，才能进行相关的操作。

二、解密及烧录方法

1、停串口

方法一：此方法主要是针对烧录了 mboot 之后，程序运行不起来并且直接进入 mboot 命令行模式。有的时候，即使在 mboot 运行正常的情况下，用 mstar 的 debug 工具也是一样的读取不到芯片的 ID 时，也可以在 secureCRT 中按住电脑的 Enter 键进入到 mboot 的命令行模式，然后输入 du 去掉关掉串口，然后再断开 secureCRT 工具。如下图：

```
<< MStar >># du
Disable UART
<< MStar >>#
```

图一

方法二：系统启动完成后关串口，这个关串口方式主要是用于研发工程师调试 PQ 或其它寄存器时使用。

在 secureCRT 中输入 00112233，最后一个 3 显示不出来才算成功，然后断开 secureCRT 工具。

（注意：当发现无法连接 mstar debug 工具的时候，可以将 secureCRT 打开，看一下板子运行的打印信息，看板子是处于哪一种状态。另外，有时候可以会遇到板子烧死的情况，即板子不停地重启，一直在跑 mboot，若遇到这种情况的话，可以让板子在上电的情况，用镊子将 flash/EMMC 的 data 线（任意两根）①短路一下，直到不重启为止，这时候再 debug 工具去连接板子）

- ① 注释：在 EMMC 左下角有左右两列平行各 4 个共 8 个电阻，对应 EMMC 的 8 根 data 线，电阻右侧连接 EMMC。操作短路时，选择任意两个电阻的右侧短接即可。如下图圆圈：



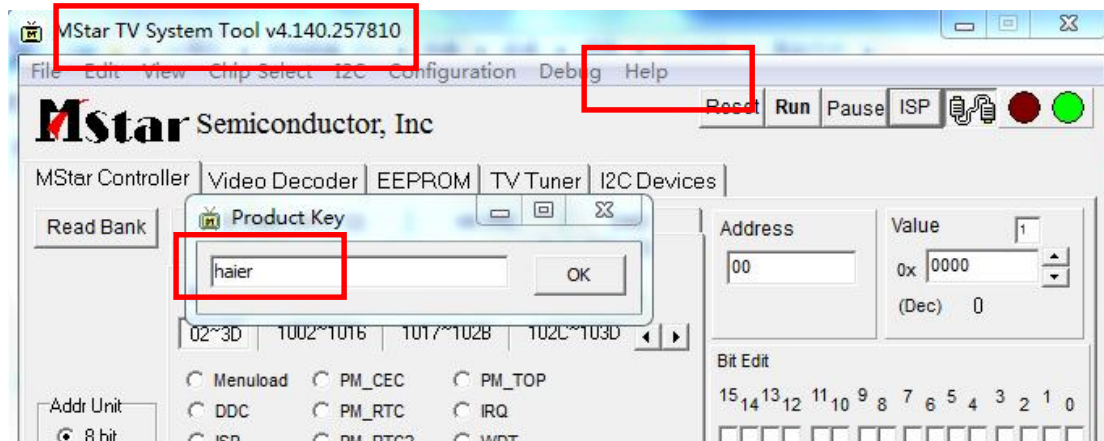
2、添加写 product key

1) 设置电脑时间

将电脑的时间改为 2010-10-30 号，日期必须是这一天的，不然 mstar debug 工具无法使用。

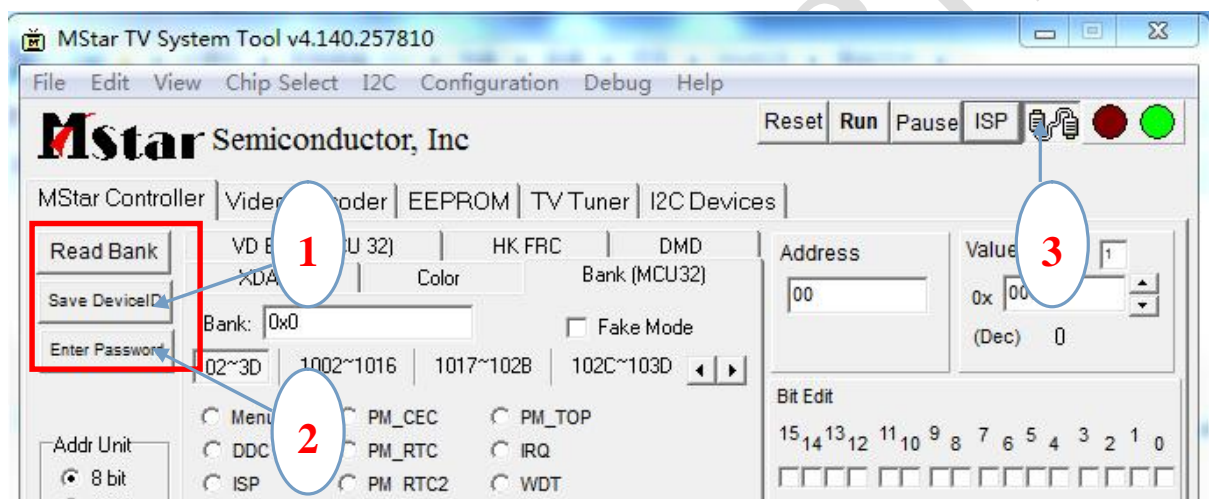
2) 解密 mstar debug 工具

Debug 工具的版本必须要是 v4.140.257810。然后点击 Help->Product Key.



图二

在弹出的窗口中输入 **haier** 后点击 OK。会出现如下图所示：



图三

3、读取 Device ID

点击上图中的 Save DeviceID 按钮，每读一次，都会将读出来的 deviceID 放在 mstar debug 工具同一级目录下的 DeviceID.txt 文件中。（最好每一片板子都读取两次，这样有便于确认 debug 工具是连接 OK，如果两次读出来的都是一样的话，那么可以说明读出来的 deviceID 是正确的，最后去整理一下，把重复的 deviceID 删除掉一个。当然这里面有另一个方法确认 deviceID 读取出来的是否正确，可以参考文档《读取设备 ID 操作文档.pdf》）

4、解密

因为每一个板子的密码都是要向 Mstar 索取，所以尽量地做到，把所有的板子的 DeviceID 都一次性读取出来，然后发给研发对应的工程师，由研发工程师向 mstar 要密钥。

研发工程师拿到密钥之后，把它放在 Password.txt 文件，这文件的格式如下：

1	69C94C540653	268E9C03412C3F6F
2	693DEA2A0AC2	CAB05E5C98B5340E
3	69105FF30C91	502196383465D392
4	69E70BCC0CB6	20EC5997F5F2D562

图四

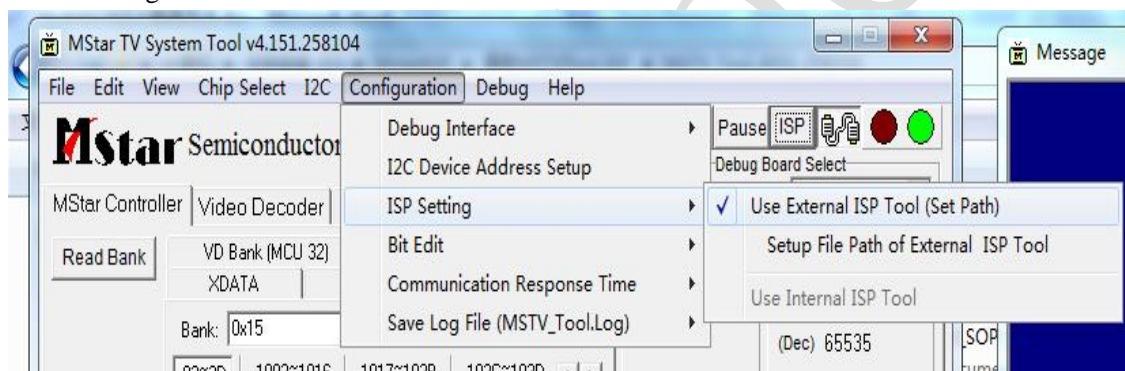
左边是 deviceID，右边是密钥，中间用空格隔开。然后把这个文件发放到工厂。

工厂拿到这个文件之后，把这文件放到 mstar debug 工具的同一级目录下。然后按照上面的操作步骤把板子连接上，点击 mstar debug 工具中的 Enter Password (图三中的步骤②) 按钮，解密成功之后，会有提示的。解密之后，把 mstar debug 工具断开 (图三中的步骤③)，也可以直接把 mstar debug 工具关掉。然后去打开 ISP 烧录工具。**(特别要注意，解密完之后的板子不能断电，若有断电操作，后面还是按上面的步骤进行解密的。)**

5、通过 ISP 工具烧录 MBOOT

1) 设置工具连接

在 debug 工具中可以直接打开 ISP 工具，设置方法如下：



点 Setup File Path of External ISP Tool 后，会弹出选择工具对话框，选选择对应的 ISP 工具即可 (ISP 工具必须是 V4.6.4.1_20140918)。

2) 用 ISP 工具烧录 MBOOT

特别注意，在解密之后，不能断电，否则 ISP 工具还是无法烧录 MBOOT。打开 ISP 工具并进行相关设置。后面操作方法跟以前 628 是一样的，在选择好文件之后，点击 connect 连接板子，连接好后再点击 run 烧录即可。