

No.18 Building, A District, No.89,  
software Boulevard Fuzhou, Fujian, PRC  
Tel: 0591-83991906-8006  
Email:zyf@rock-chips.com

# **Rockchip Secure Boot Application Note**

**Revision1.2**

**2016/02/02**



## Revision History

| Revision | Date       | Description | Author |
|----------|------------|-------------|--------|
| 1.0      | 2014-11-05 | 初版.         | ZYF    |
| 1.1      | 2015-12-21 | 更新          | Ybc    |
| 1.2      | 2016-02-02 | 更新          | YHC    |

目录:

1. 基础信息
2. SecureBoot 原理
3. 固件签名
4. Efuse 烧录
5. 固件升级和测试
6. 常见问题

## 1. 基础信息

本文档支持平台有 RK3126、RK3128、RK3228、RK3288 RK3368.

Rockchip Secure Boot 解决方案的特性:

1.1 支持 Secure Boot Rom

1.2 支持 SHA256 或者 SHA160

1.3 支持 RSA2048 或者 RSA 1024

1.4 支持 OTP 验证 RSA Public Key

1.5 支持 Secure Boot Rockusb 升级固件

相关工具和 loader 版本:

1、 Miniloader 版本需要 2.19 或更新版本

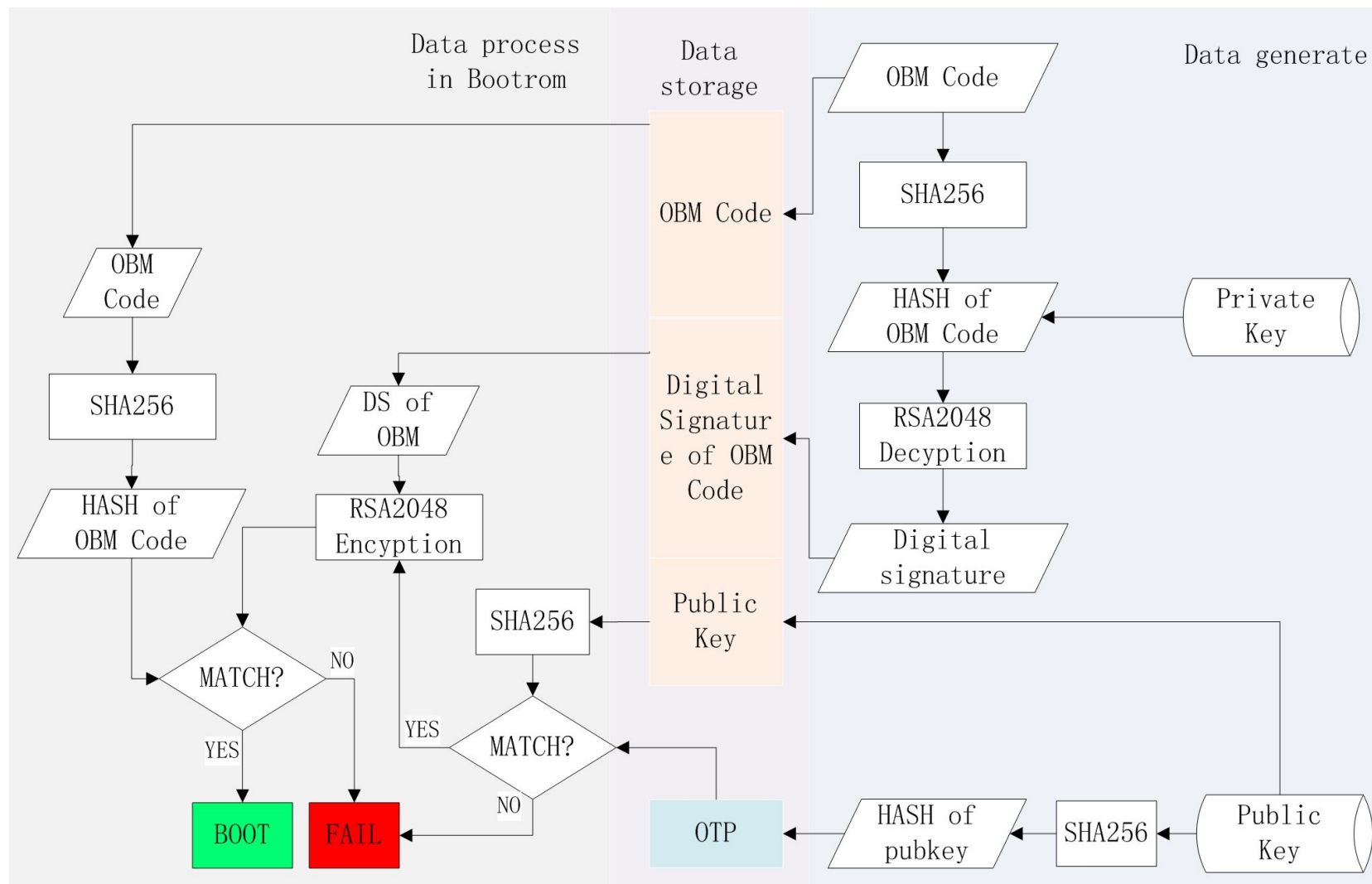
2、 Uboot 版本需要 2.17 或者更新版本

3、 Efuse 工具版本 1.35 或者更新版本

4、 SecureBootTool 版本需要 1.75 或者更新版本

5、 RKBatchTool 版本需要 1.8 或者更新版本

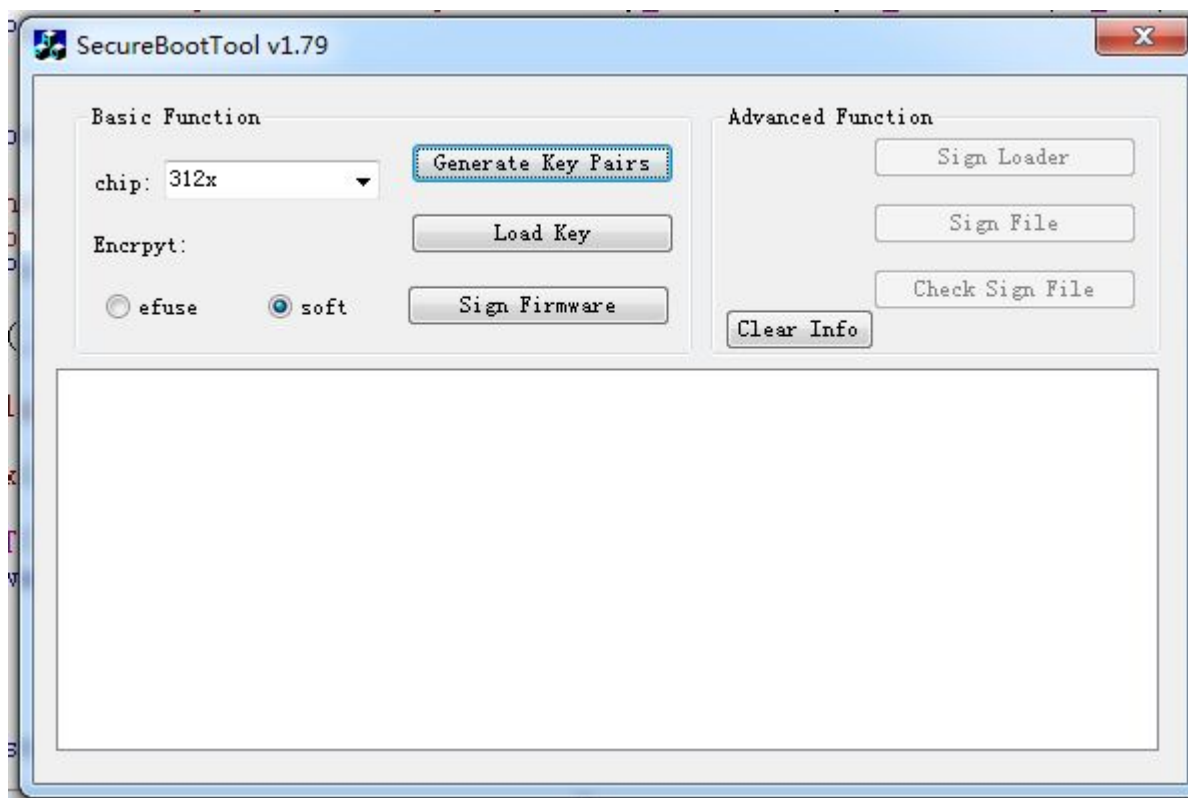
## 2. SecureBoot 原理



### 3. 固件签名

这个是 WIN 平台下的说明，LINUX 下的参考工具自带文档。

#### 3.1 签名工具界面：



### 3.2 配置说明:

chip: 312x

: 选择芯片型号, 3188 之前的芯片选择 others

Encrypt:  
☐ efuse ☒ soft

: 配置加密类型是写 efuse 加密还是软件加密 (注: 3128, 3288, 3228, 3368 支持 efuse 级加密, 其他的旧芯片不支持)。

Generate Key Pairs

: 生成 RSA KEY, 每款机器只能生成一次, 请一定备份好 KEY, 如果丢失, 那么机器将不能再更新固件。

Load Key

: 加载之前备份的 RSA KEY (工具支持 openssl 生成的.pem 的 2048key)。

Sign Firmware

: 签名固件。

关于芯片 config 配置:

#### [Options]

#3188 以及之前其他旧芯片 使用 loaderex 为 false, key 为 1024;

#3128, 3288, 3228, 3368 loaderex 为 true , key 为 2048, 但是需要确认一下几个点:

# (1) 需要 minloader2.19 或者更新版本

# (2) 需要 Uboot 2.17 或者更新版本

# (3) 需要 key 2048

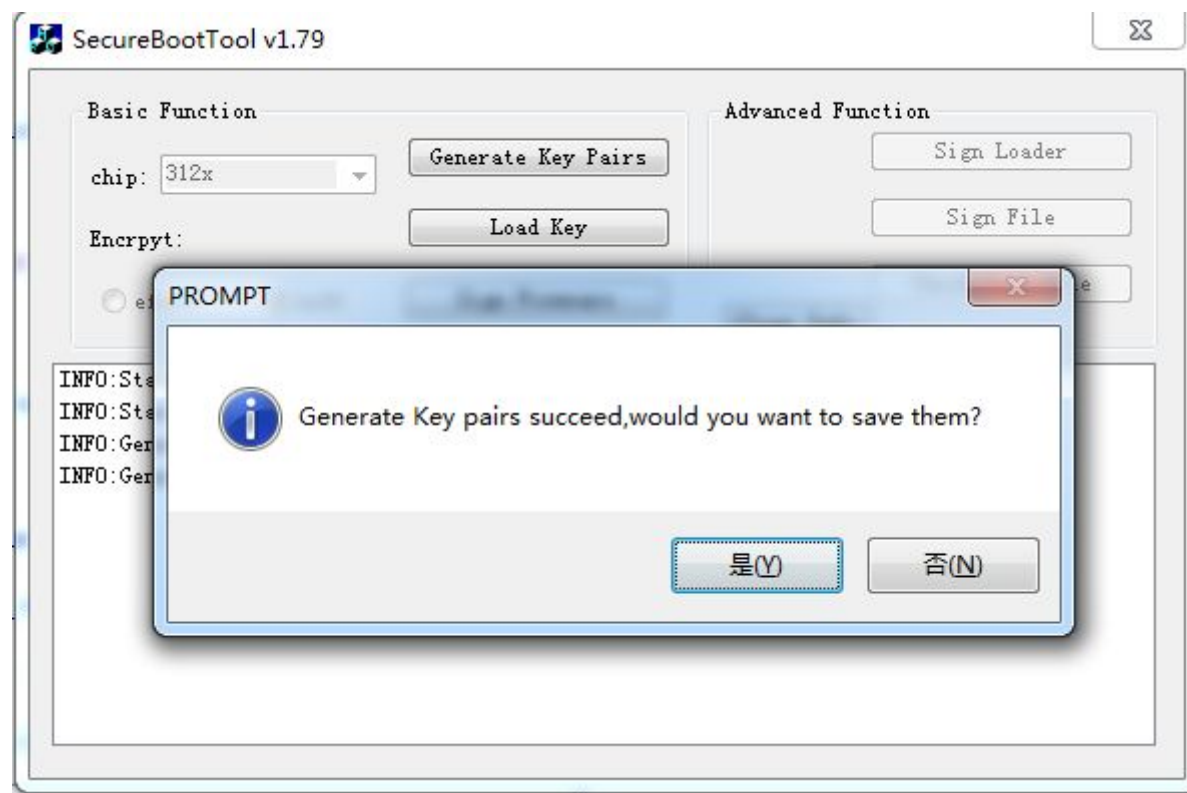
**Loaderex=true**

#只支持 1024、2048 两种

**Key=2048**

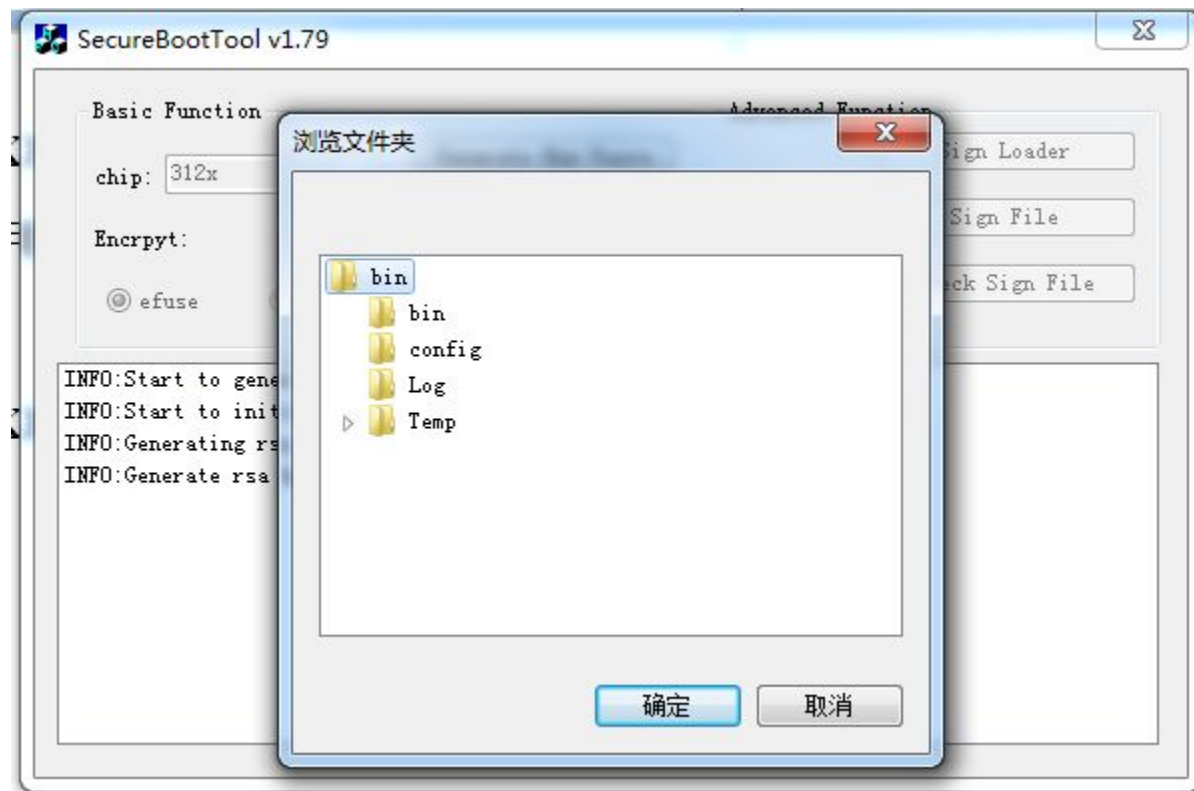
**3.3 生成 RSA KEY，每款机器只生成一次**



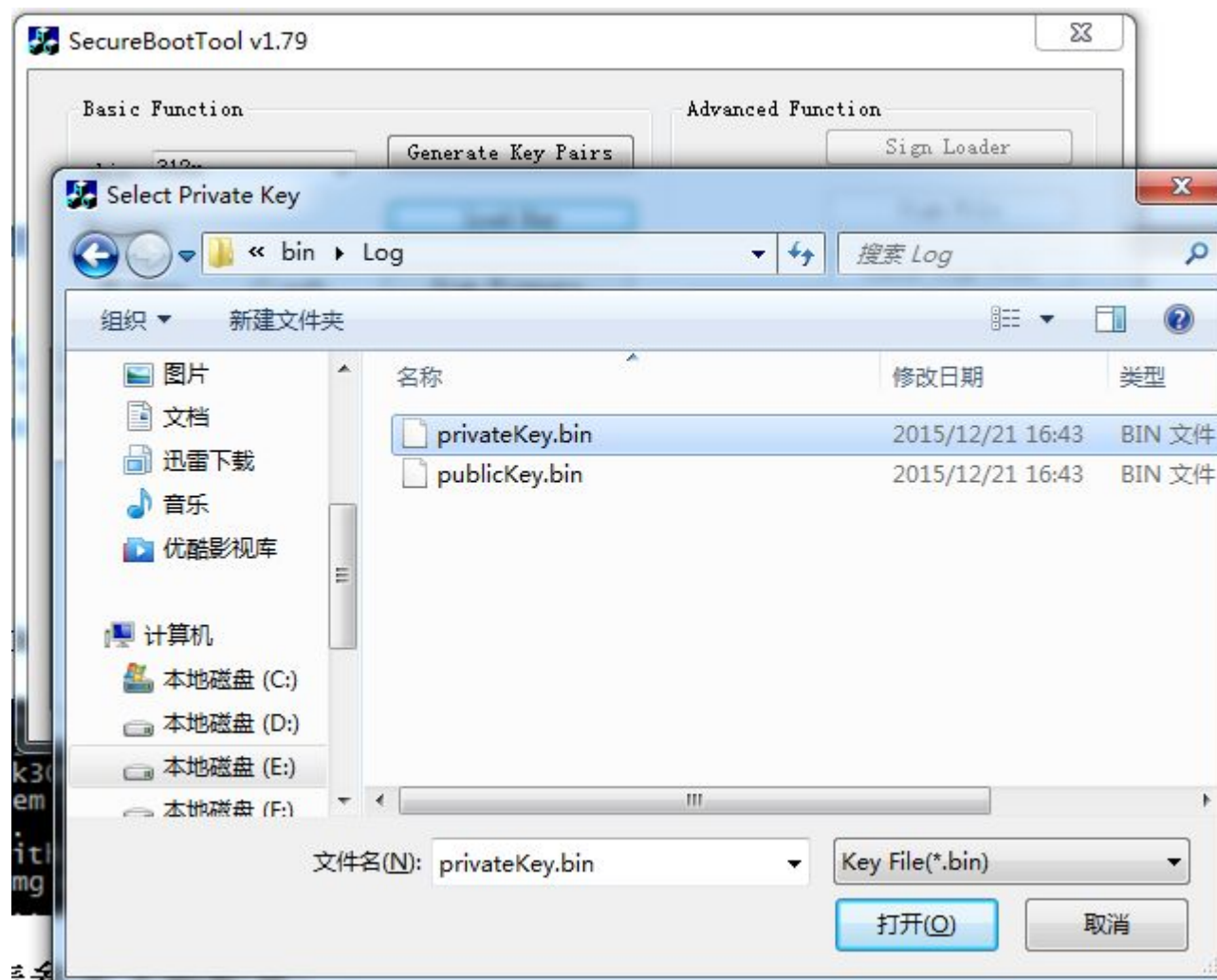


### 3.4 保存 RSA KEY.

以后签名都只用这对 KEY，建议最好再备份一次，避免丢失。



### 3.5 加载 RSA KEY



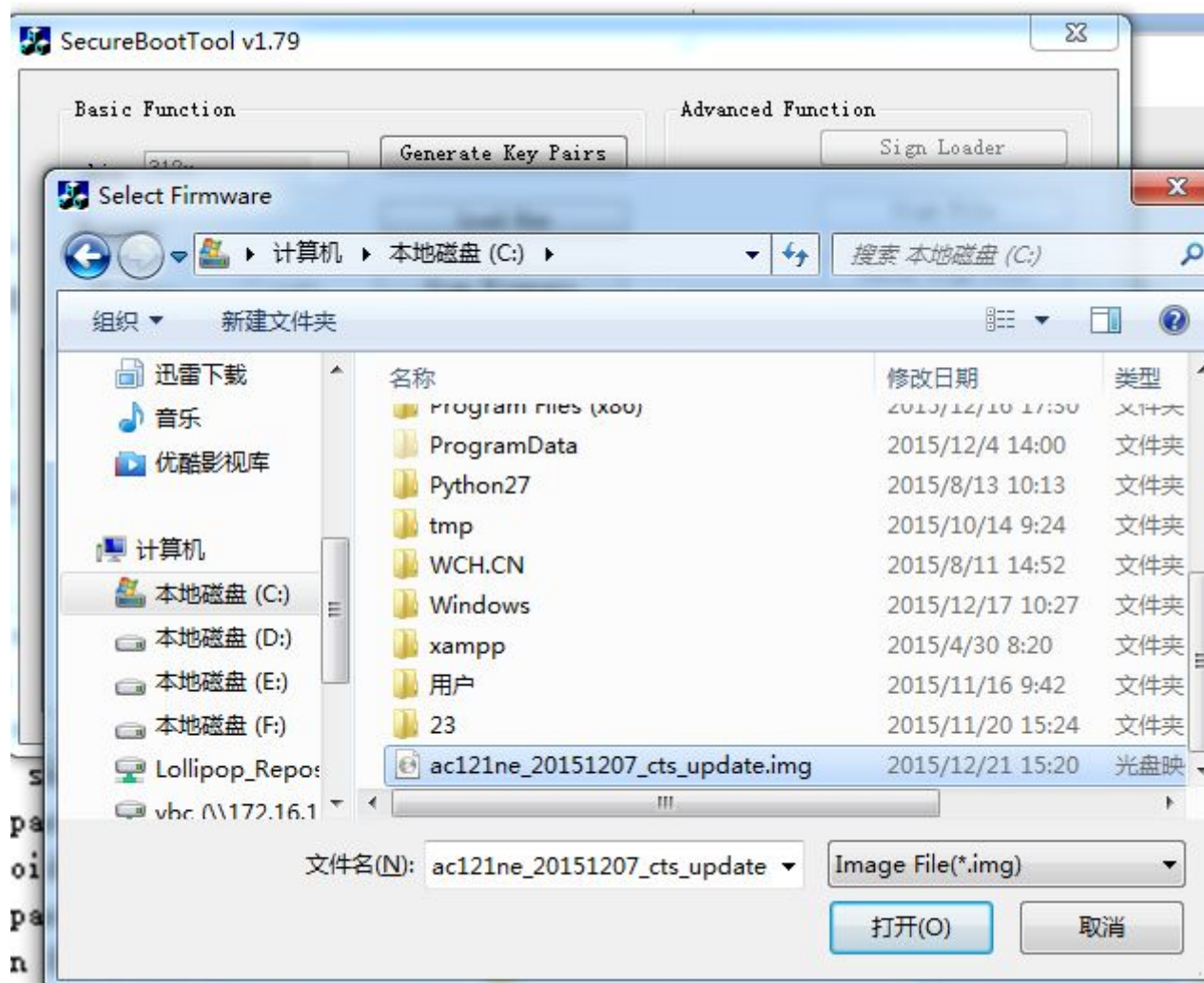
### 3.5 签名固件

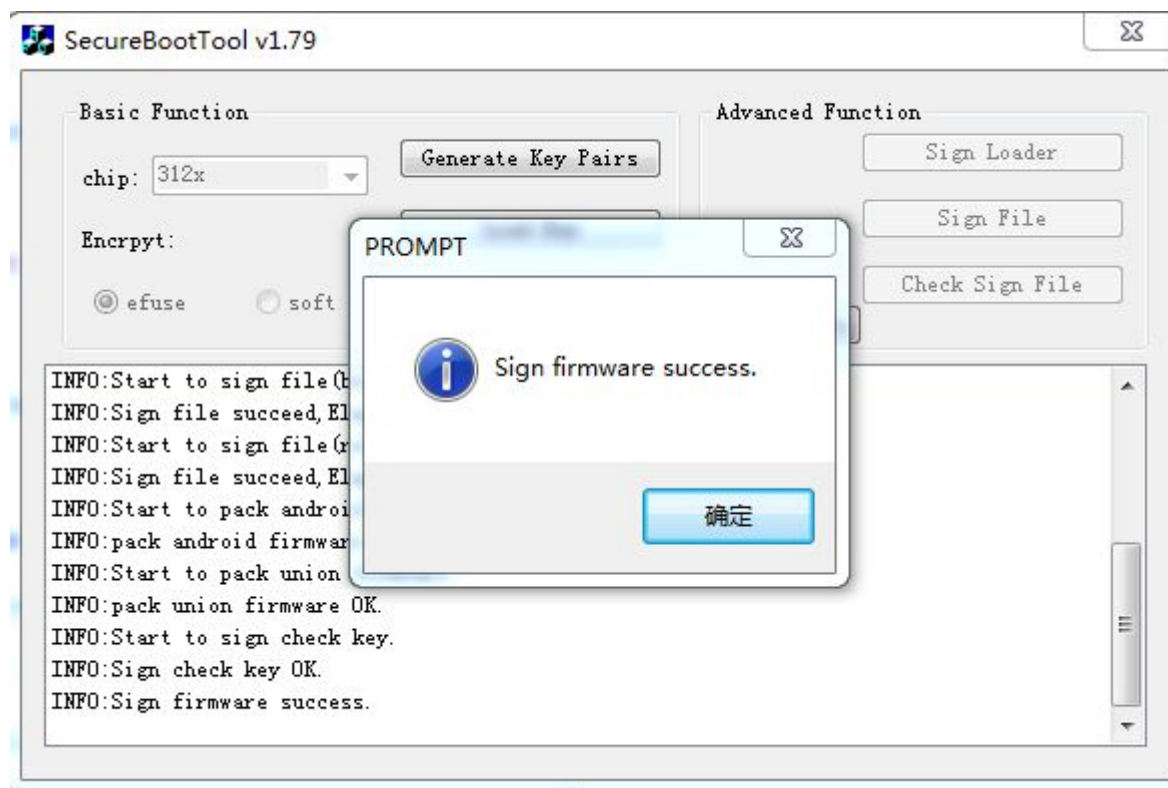
固件要求 boot.img 和 recovery.img 都需要包含 kernel.参考下面命令.

```
zyf@fs-server:~/rk30/rk3288_android4.4$ ./mkimage.sh ota
TARGET_PRODUCT=rk3288
TARGET_HARDWARE=rk30board
system filesystem is ext4
make ota images...
create boot.img with kernel... done.
create recovery.img with kernel... done.
create misc.img... done.
```

注意:使用 nand flash 时,打包的固件里面需要包含 miniloader 和 uboot.img.uboot 的编译参考 uboot 开发文档。

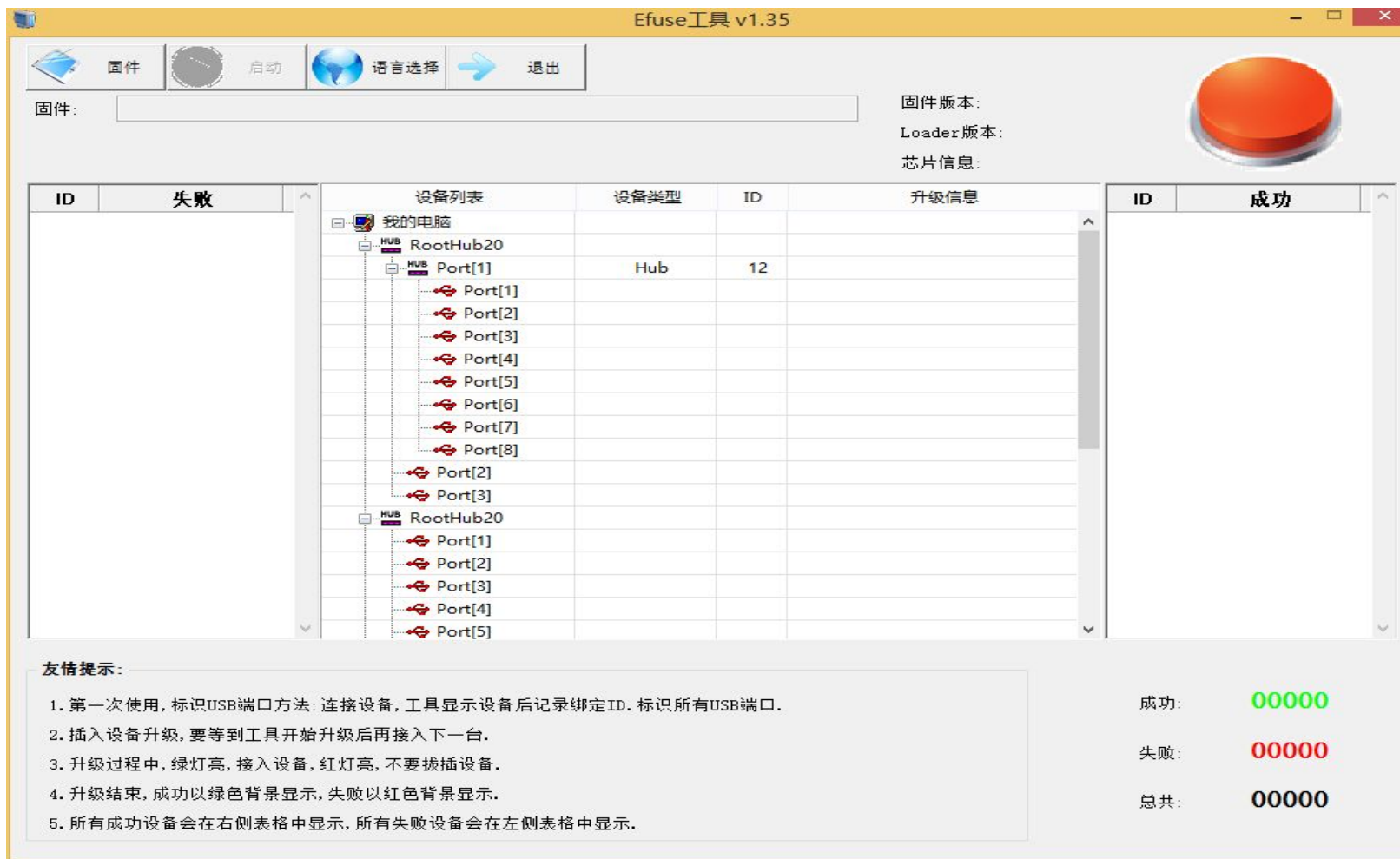
签名固件:





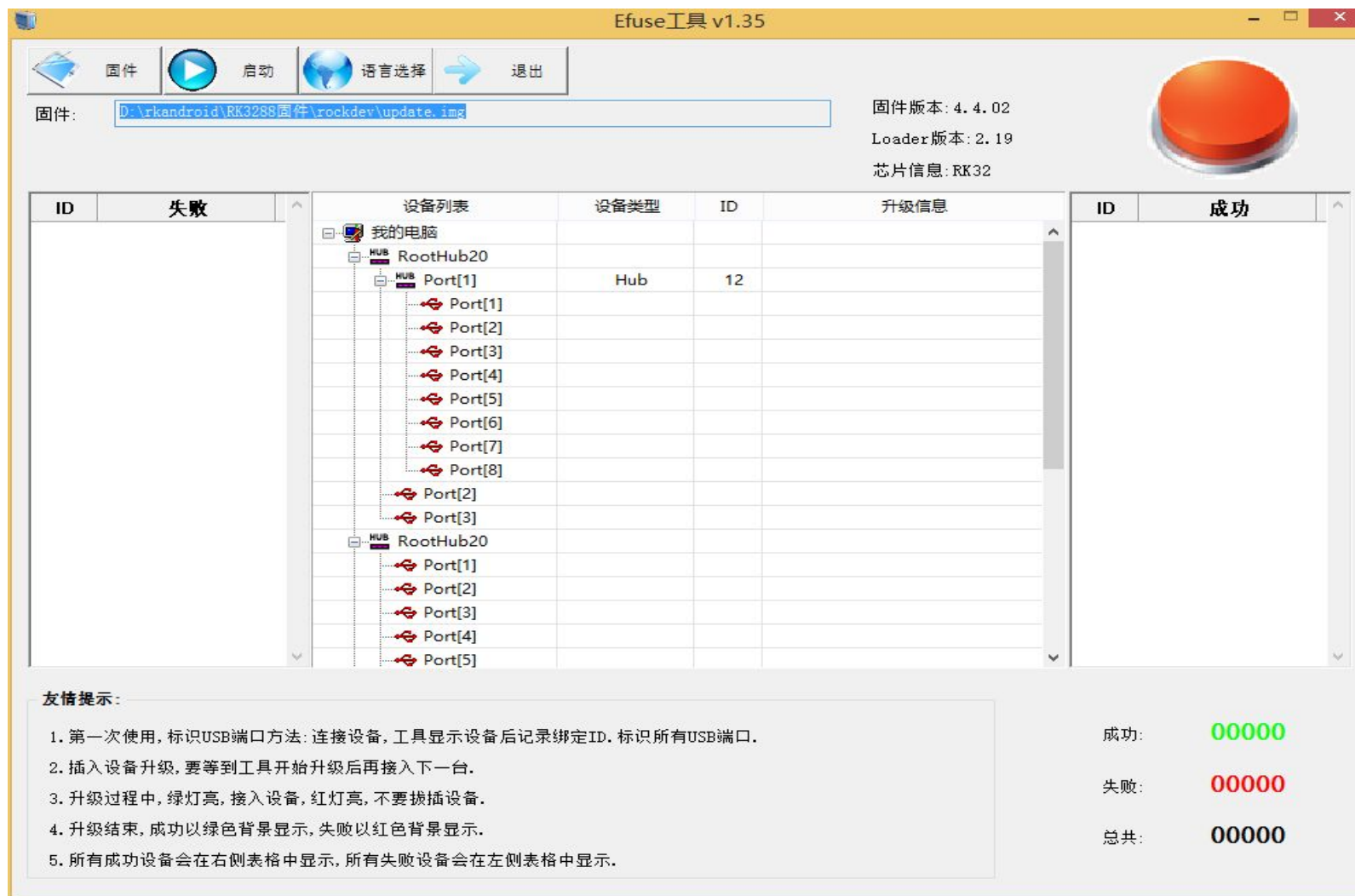
## 4. 烧写 Efuse

### 4.1 工具界面



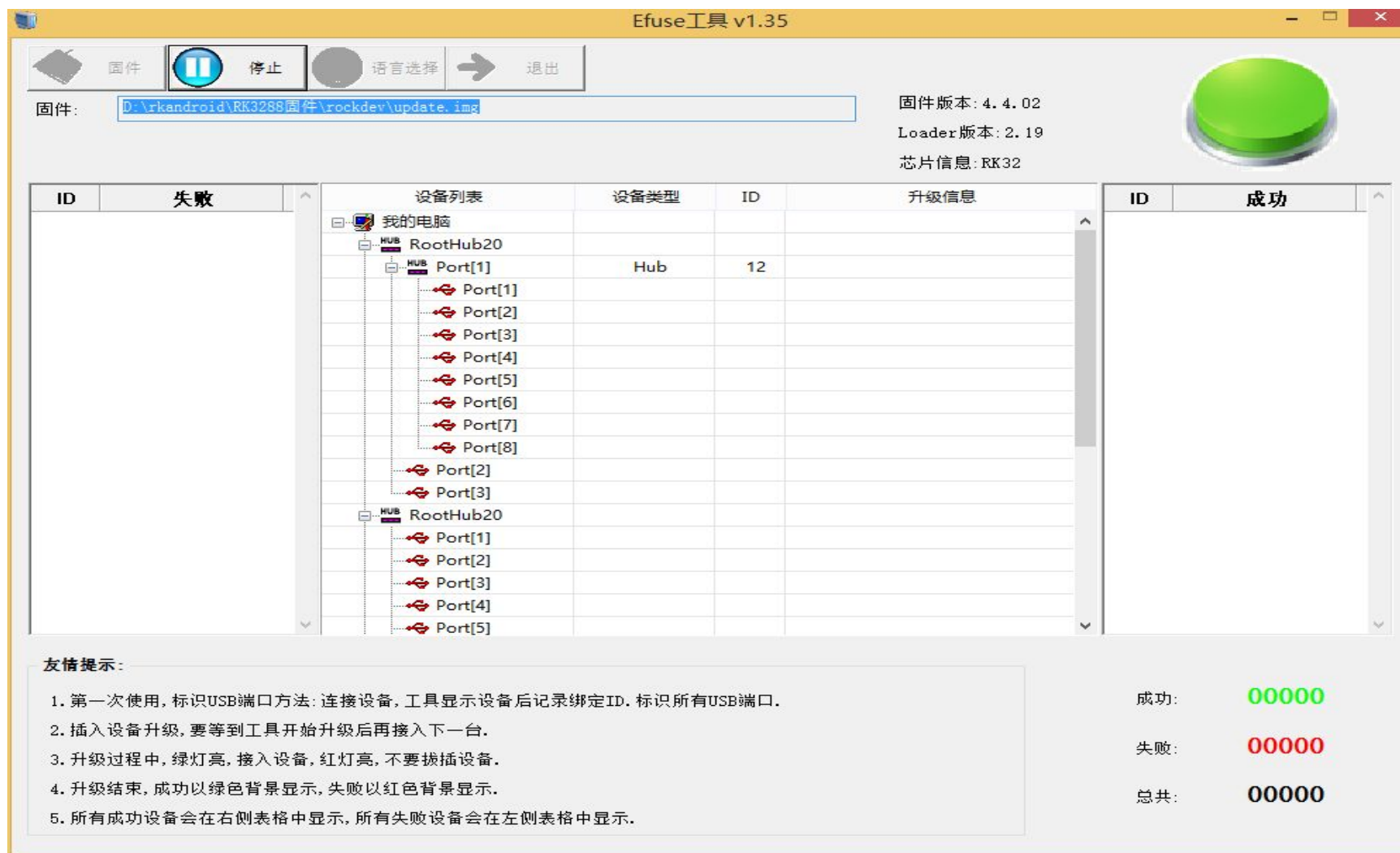
## 4.2 选择签名过的固件（用于生产的固件）





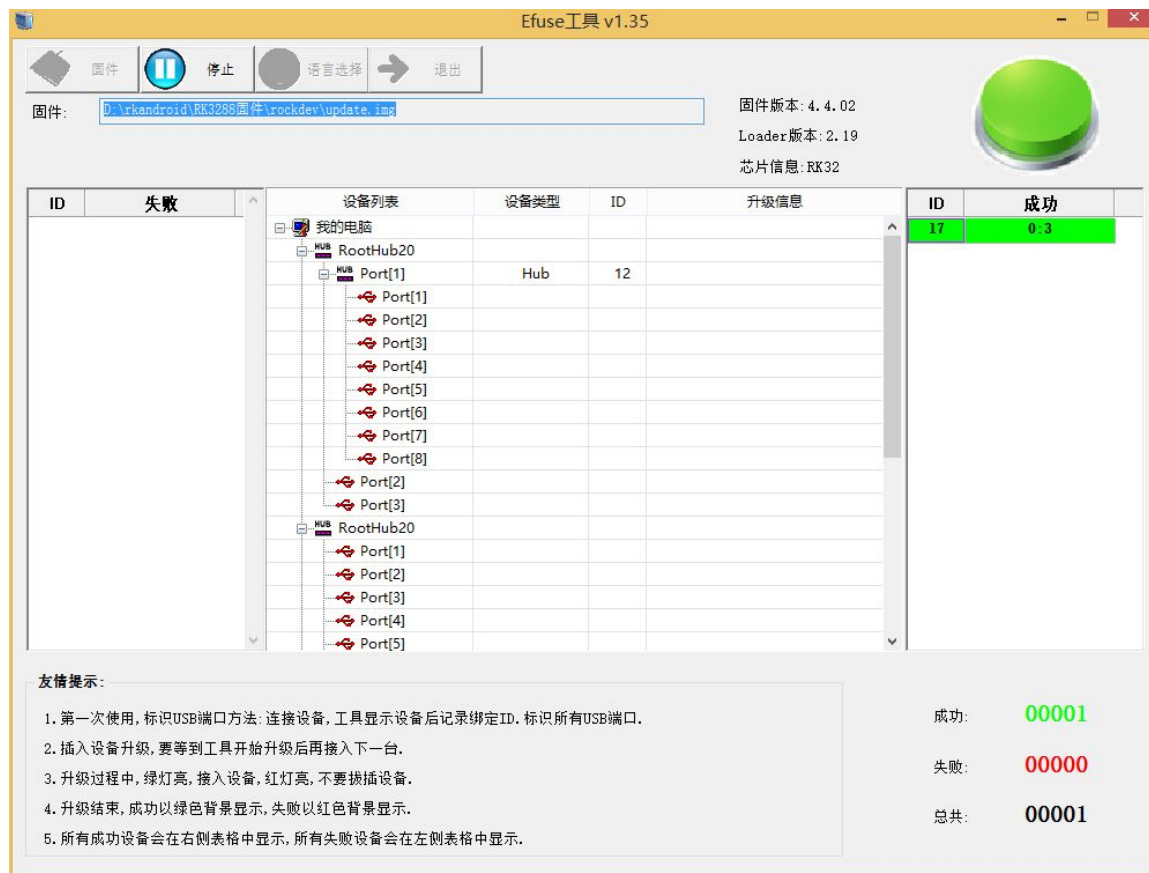
## 4.3 点击“启动”按钮





## 4.4 烧录 EFUSE

裸机开机接 USB 会进入 “maskromrockusb” 升级模式，工具会自动烧写 EFUSE,工具支持一拖多烧录。



**注意事项:**

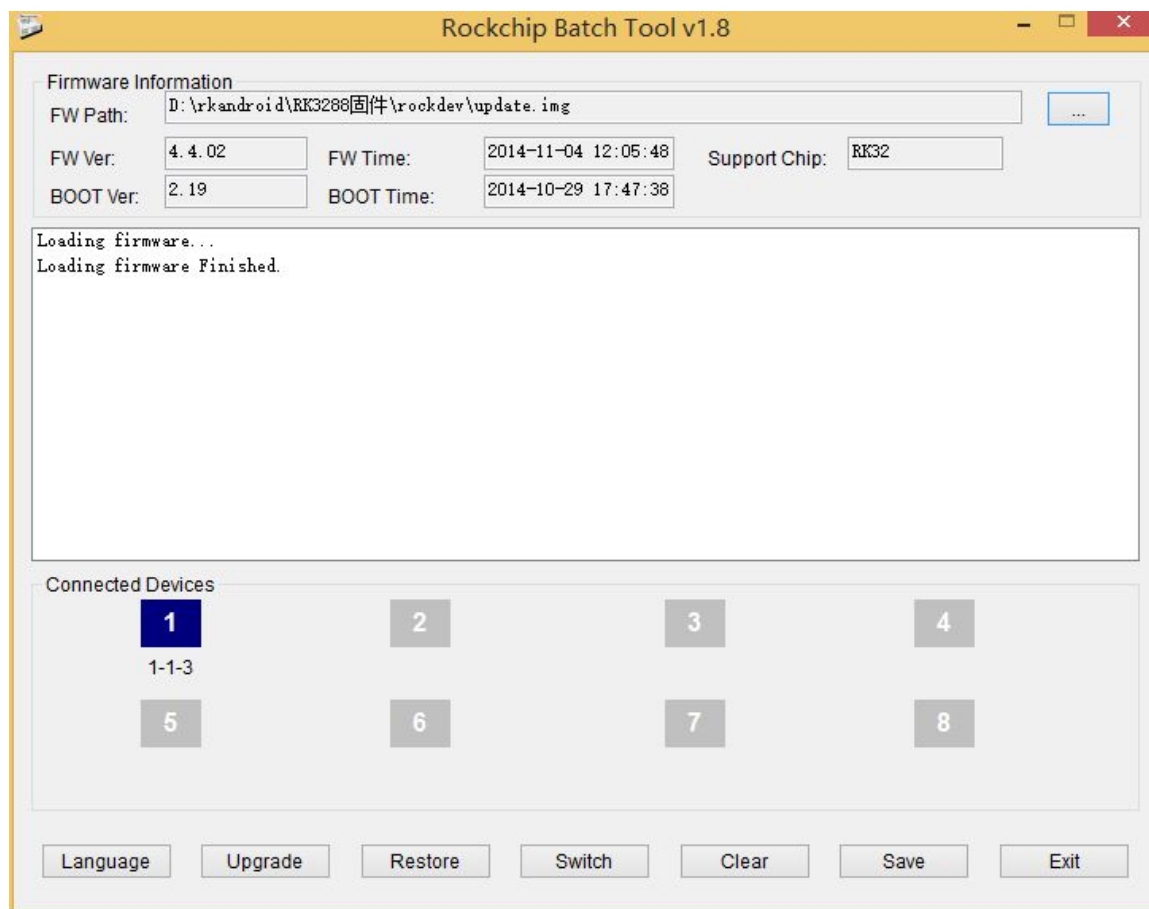
- 1、RK312X 需要使用治具，EFUSE 需要单独供电才能烧录
- 2、RK3288 PCBA 上已经有 EFUSE 已经有供电，烧录软件会自动控制，不需要单独供电
- 3、批量烧录前先烧录一台机器，然后用量产工具升级完整固件，确认所有功能正常后再开始批量烧录。

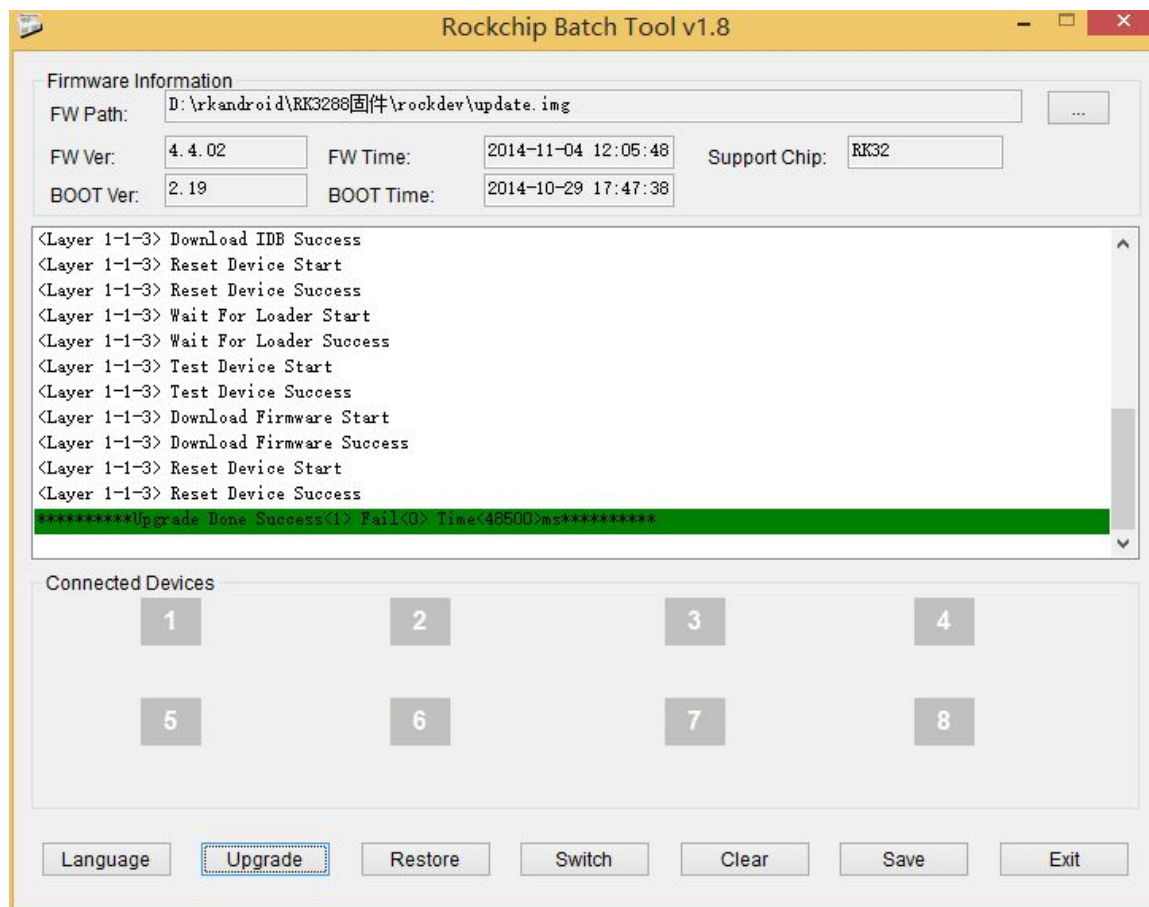
**警告：RSA EKY 一定要备份，不然机器可能变砖或者不能再次更新固件。**

## 5 固件烧录和测试

## 5.1 用最新的量产工具升级签名过的固件

机器需要先烧录 EFUSE，如果没有烧录 EFUSE，那么机器将不会启用 Secure Boot。

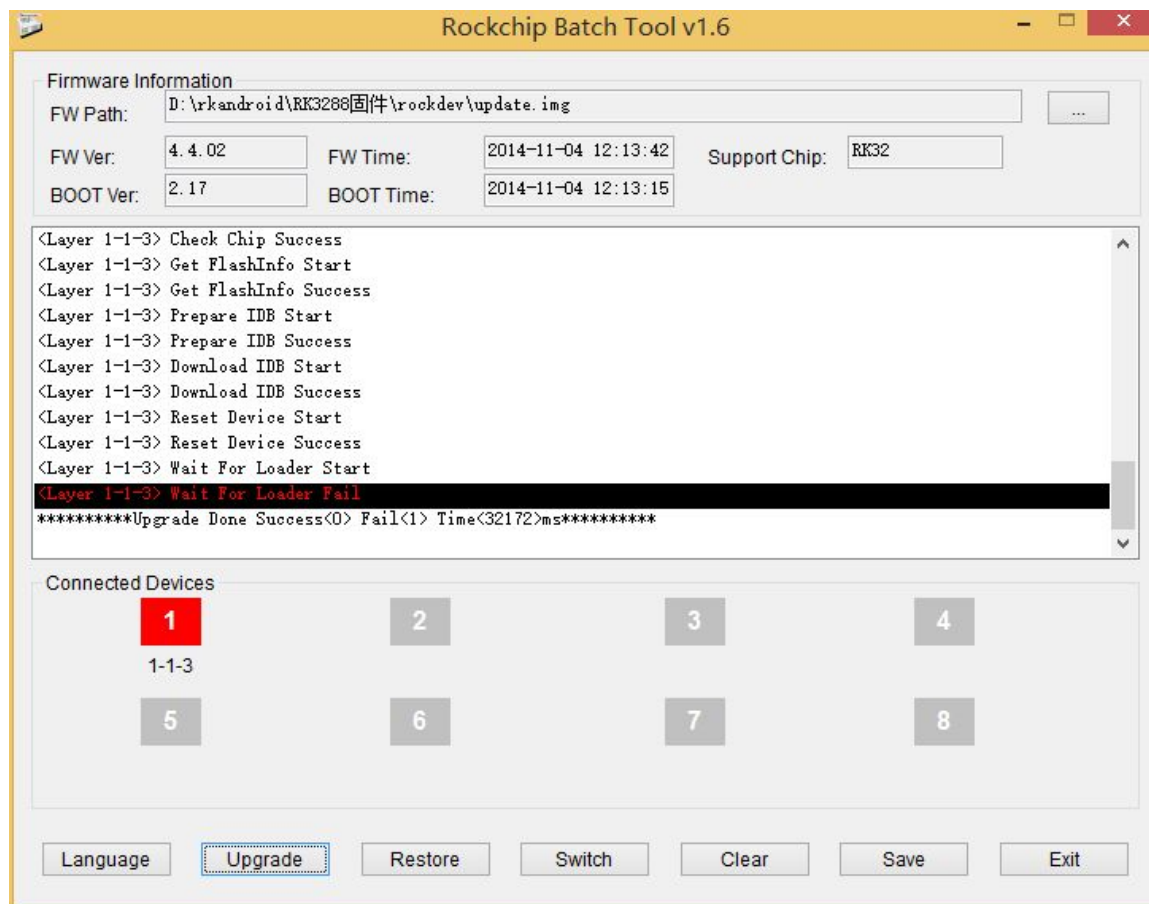




## 5.2 验证

用量产工具烧录没有签名的固件，机器将不能启动，停留在“maskromrockusb”升级模式。

升级完 loader 后工具会直接报错:



## 6. 常见问题处理

### 6.1 Efuse 烧录出错

检查 Efuse 供电是否正常

检查机器是否已经烧录过