

密级状态：绝密() 秘密() 内部() 公开(√)

Rockchip_Secure_Boot_Application _Note

(技术部，第二系统产品部)

文件状态： [] 正在修改 [√] 正式发布	当前版本：	V1.2.1
	作 者：	卞金晨
	完成日期：	2017-11-22
	审 核：	
	完成日期：	

福州瑞芯微电子股份有限公司

Fuzhou Rockchips Electronics Co. , Ltd

(版本所有,翻版必究)

版 本 历 史

版本号	作者	修改日期	修改说明	备注
V1.0	ZYF	2014-11-05	初版	
V1.1	Ybc	2015-12-21	更新	
V1.2	Yhc	2016-02-02	更新	
V1.2.1	卞金晨	2017-11-28	修订适配 Android Oreo	

目 录

概述.....	1
1. SECURE BOOT 原理.....	2
2. 生成 UPDATE.IMG.....	2
2.1 生成镜像.....	2
2.2 制作 UPDATE.IMG.....	2
3. 固件签名.....	4
3.1 生成 RSA 密钥.....	4
3.2 加载 RSA KEY.....	5
3.3 配置工具.....	6
3.4 签名固件.....	7
4. 烧写 EFUSE.....	8
4.1 工具界面.....	8
4.2 选择签名过的固件（用于生产的固件）.....	8
4.3 点击“启动”按钮.....	8
4.4 烧录 EFUSE.....	8
5. 固件烧录和测试.....	9
5.1 用最新的量产工具升级签名过的固件.....	9
5.2 验证.....	9
6. 常见问题处理.....	10
6.1 EFUSE 烧录出错.....	10

概述

本文档适用于 RK3126, RK3128, RK3228, RK3229, RK3288, RK3368, RK3399, RK3228H 和 RK3328。

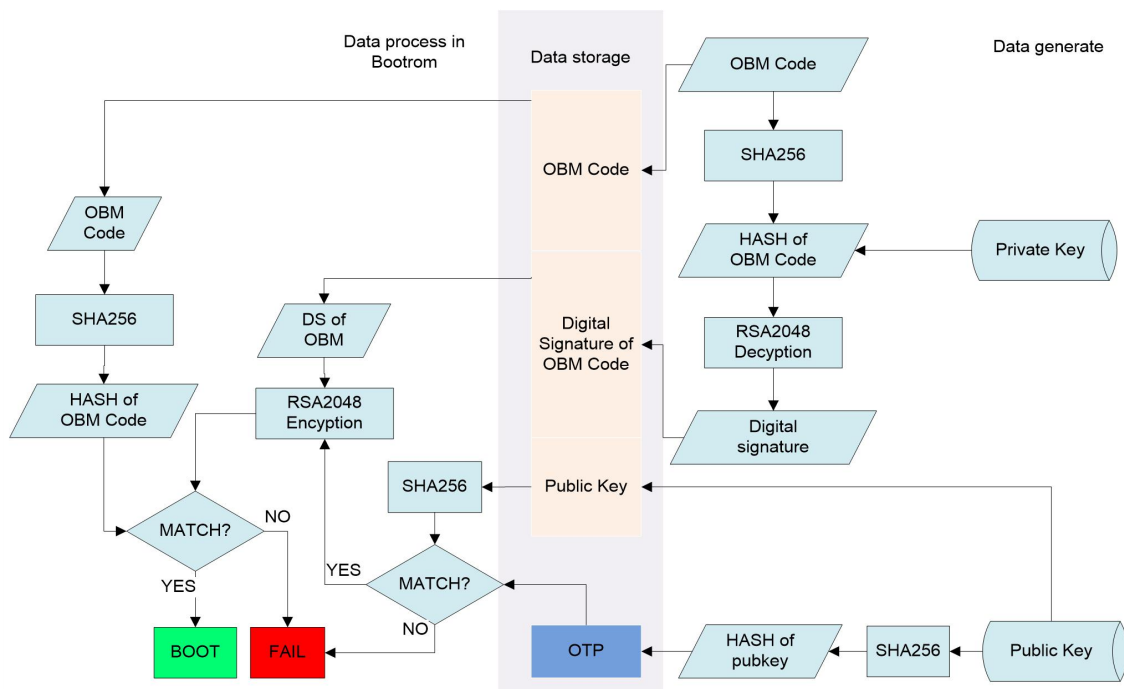
Rockchip Secure Boot 解决方案的特性:

- 支持 secure boot ROM
- 支持 SHA256
- 支持 RSA2048
- 支持 OTP 验证 RSA 公钥
- 支持 Secure Boot Rockusb 升级固件

相关工具和 loader 版本要求:

- Miniloader 需要 V2.19 或更新版本
- Uboot 需要 V2.17 或更新版本
- BL31 (trust) 需要 V2.17 或更新版本
- Efuse 工具需要 V1.35 或更新版本
- SecureBootTool 需要 V1.79 或更新版本
- RKBatchTool 需要 V1.8 或更新版本(已弃用, 使用工厂工具替代)
- FactoryTool 需要 V1.39 或更新版本

1. Secure Boot 原理



2. 生成 Update.img

2.1 生成镜像

编译 Android 后，使用如下脚本生成镜像：

./mkimage.sh ota

```
projects@bogon:~/release/RK3288/mid/5.1$ ./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.
create system.img... done.
```

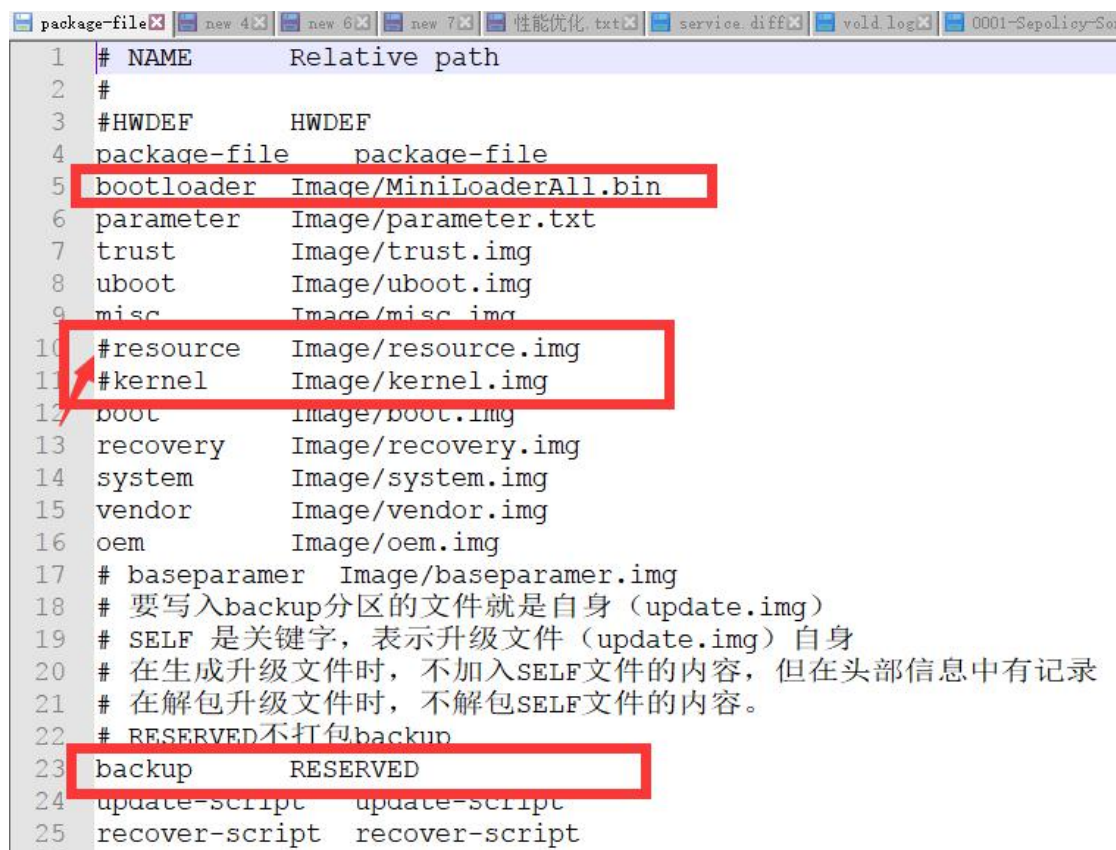
Figure 2-1 生成镜像的脚本

2.2 制作 Update.img

配置文件位于 RKTools/windows/AndroidTool/rockdev/package-file，这个文件控制哪些镜像需要打包进去；

以 3368 为例，更改 bootloader 的路径，注释掉 resource 和 kernel，设置 backup

为 RESERVED;



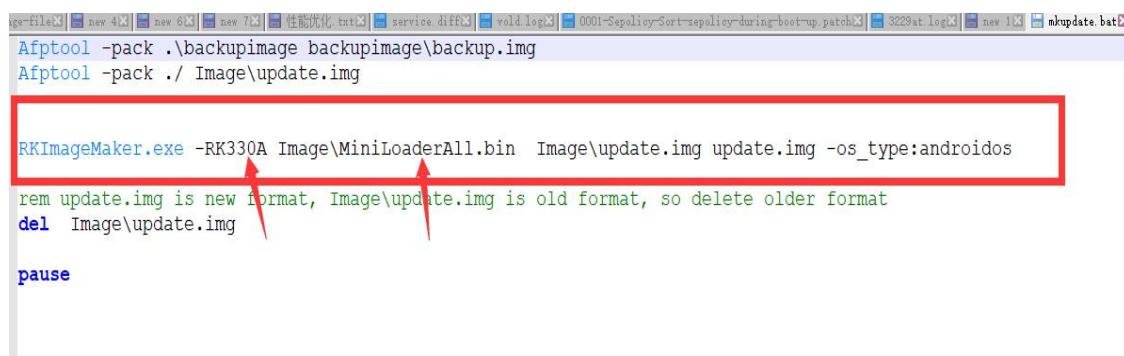
```

1 # NAME      Relative path
2 #
3 #HWDEF      HWDEF
4 package-file package-file
5 bootloader Image/MiniLoaderAll.bin
6 parameter  Image/parameter.txt
7 trust      Image/trust.img
8 uboot      Image/uboot.img
9 misc       Image/misc.img
10 #resource   Image/resource.img
11 #kernel     Image/kernel.img
12 boot       Image/boot.img
13 recovery   Image/recovery.img
14 system     Image/system.img
15 vendor     Image/vendor.img
16 oem        Image/oem.img
17 # baseparamer Image/baseparamer.img
18 # 要写入backup分区的文件就是自身 (update.img)
19 # SELF 是关键字, 表示升级文件 (update.img) 自身
20 # 在生成升级文件时, 不加入SELF文件的内容, 但在头部信息中有记录
21 # 在解包升级文件时, 不解包SELF文件的内容。
22 # RESERVED不打包backup
23 backup     RESERVED
24 update-script update-script
25 recover-script recover-script
  
```

Figure 2-2 打包用到的配置文件

复制 RKTools/windows 文件夹到 windows 系统中, 然后执行 AndroidTool/rock dev/mkupdate.bat 脚本来生成 update.img.

注意:上述脚本中的平台需要修改, 具体可以使用工厂工具读取后设置。



```

Afptool -pack .\backupimage backupimage\backup.img
Afptool -pack ./ Image\update.img

RKImageMaker.exe -RK330A Image\MiniLoaderAll.bin Image\update.img update.img -os_type:androidos
rem update.img is new format, Image\update.img is old format, so delete older format
del Image\update.img

pause
  
```

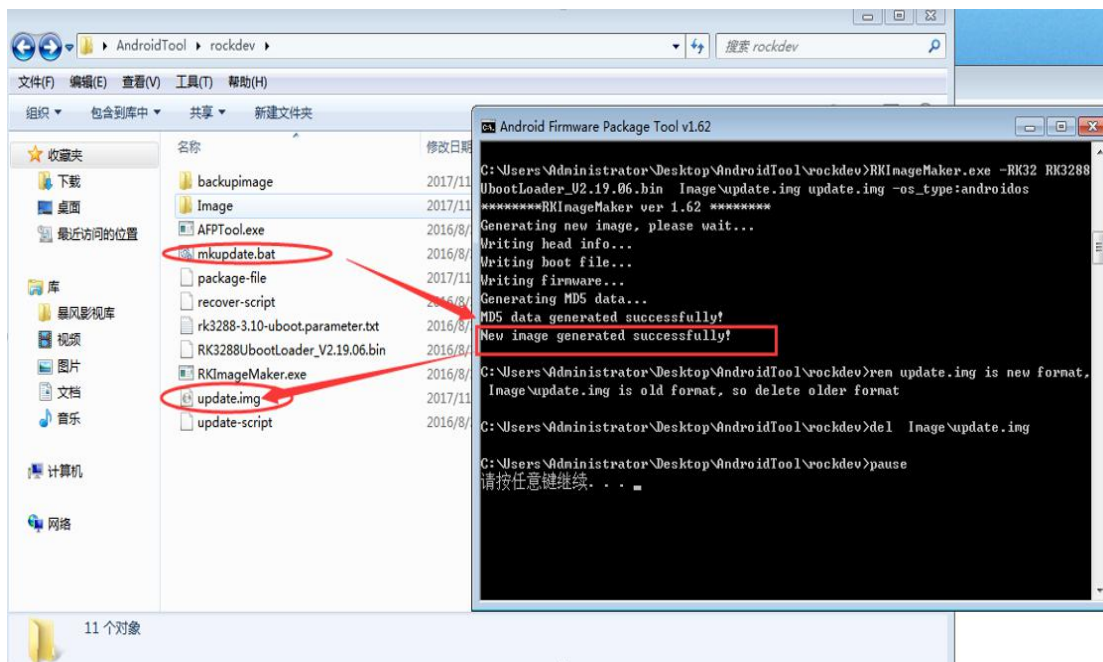


Figure 2-3 执行 Win 脚本

3. 固件签名

本文档是针对 Win 平台的说明，Linux 请参考自带文档。

3.1 生成 RSA 密钥

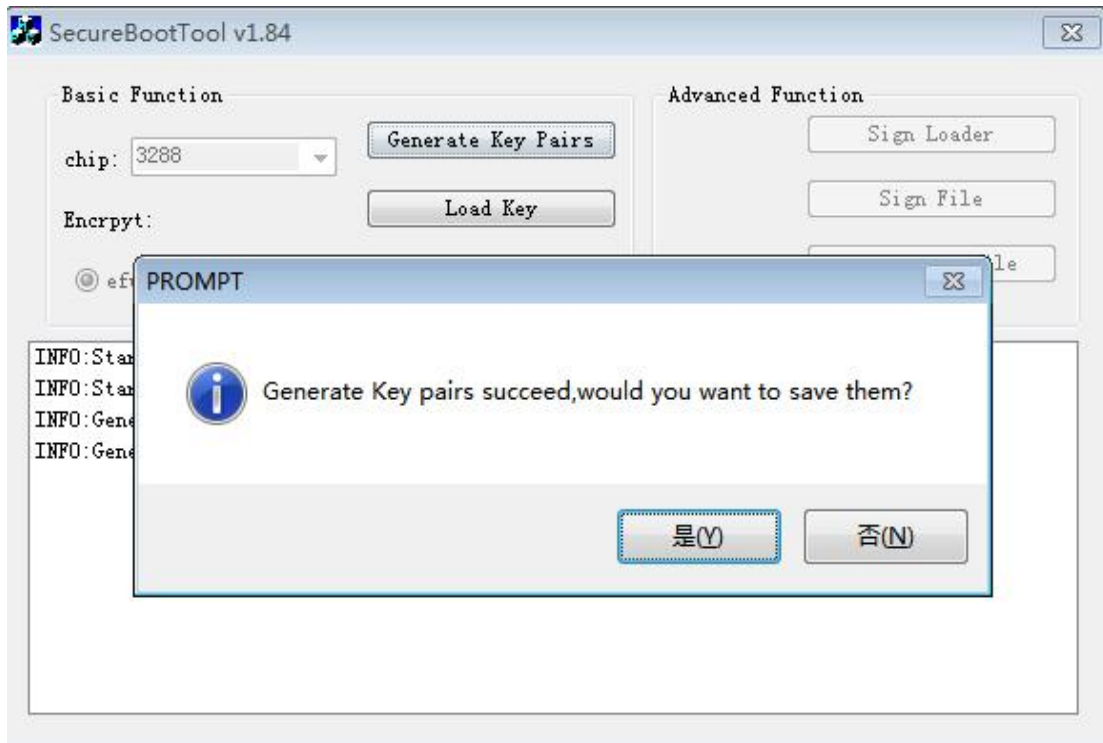


Figure 3-1 SecureBootTool 生成 RSA 密钥

妥善保存 RSA 密钥文件，这对密钥将用于对固件的签名以及 OTA 升级，请务必备份到可靠的地方。

注意：这对密钥文件非常重要，请确保不会丢失，一旦丢失或损坏，后续将永久无法升级或刷写固件。

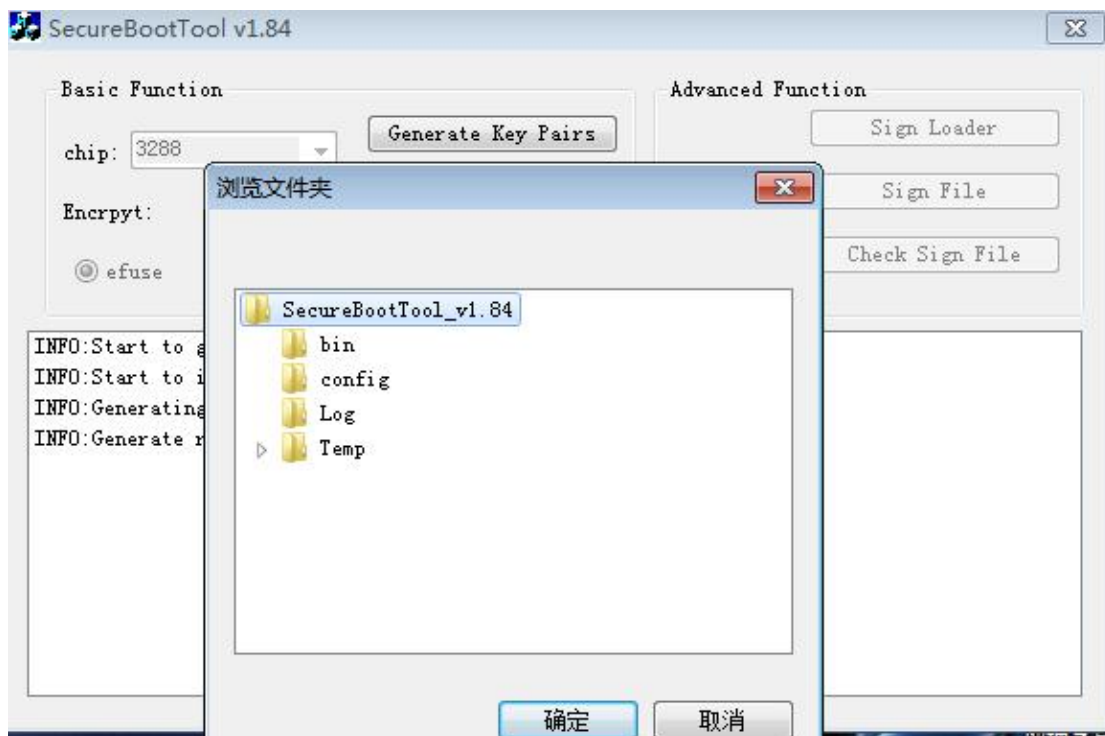


Figure 3-2 保存 RSA key

3.2 加载 RSA key

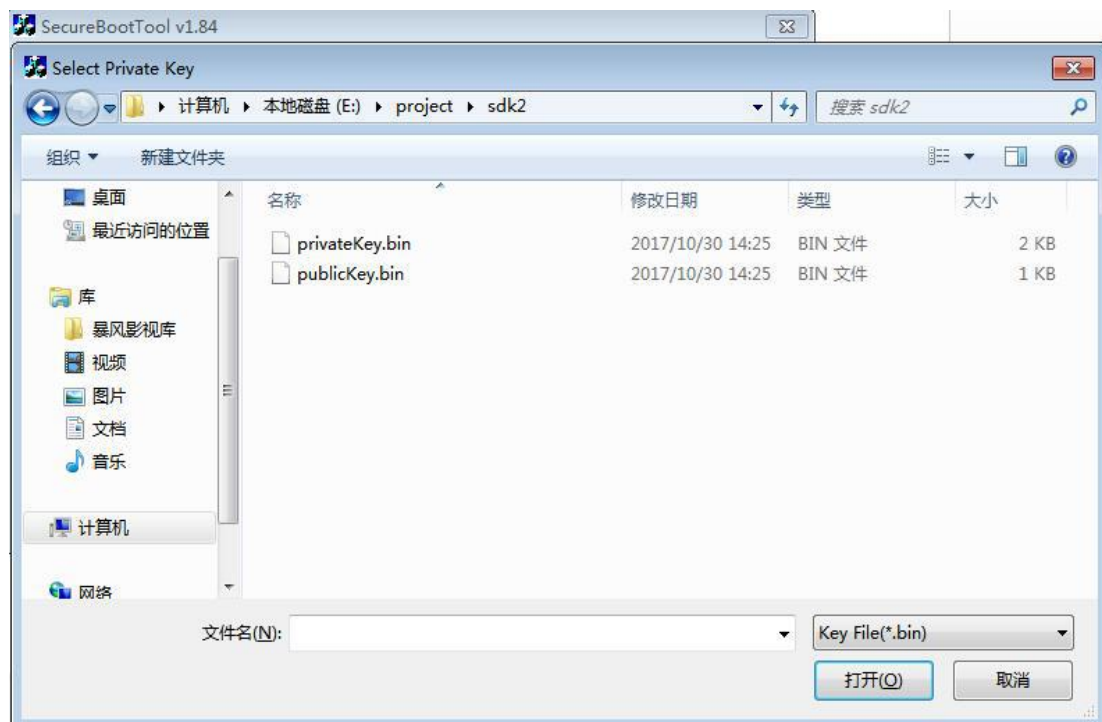
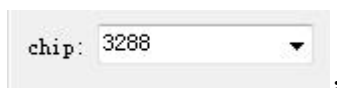


Figure 3-3 加载 RSA key

3.3 配置工具



选择平台：

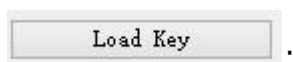


'efuse' 选项意味着将烧写公钥的哈希到设备的 eFuse 中，将启用 secure boot ROM(推荐)；

'soft' 选项针对一些特殊的程序，不会启用 secure boot ROM，使用 RSA1024 and SHA160；



每款产品只生成一次 RSA KEY，务必备份好以免无法升级或烧写固件；



加载备份的 RSA key (支持使用 openssl 生成的'.pem'文件)；



签名固件；

注意：右侧的隐藏功能需要使用组合键：**Ctrl + ALT+ R + K**，用于签名单独 Loader 或其他文件等。

3.4 签名固件

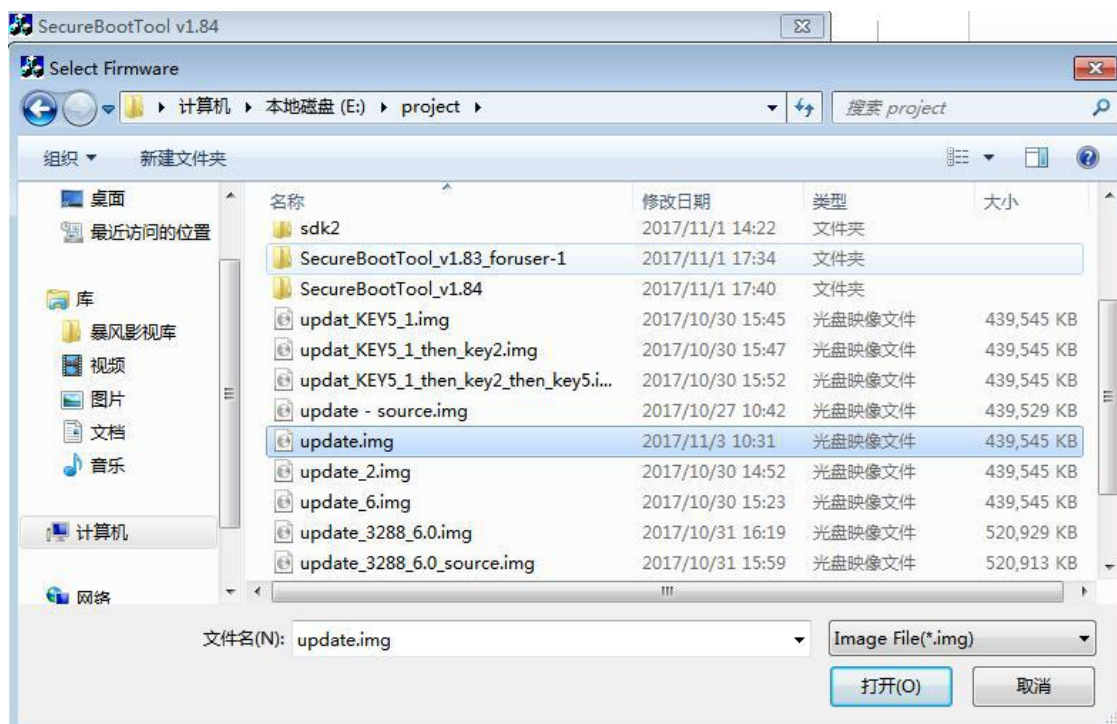


Figure 3-4 SecureBootTool 选择固件

Signed firmware:

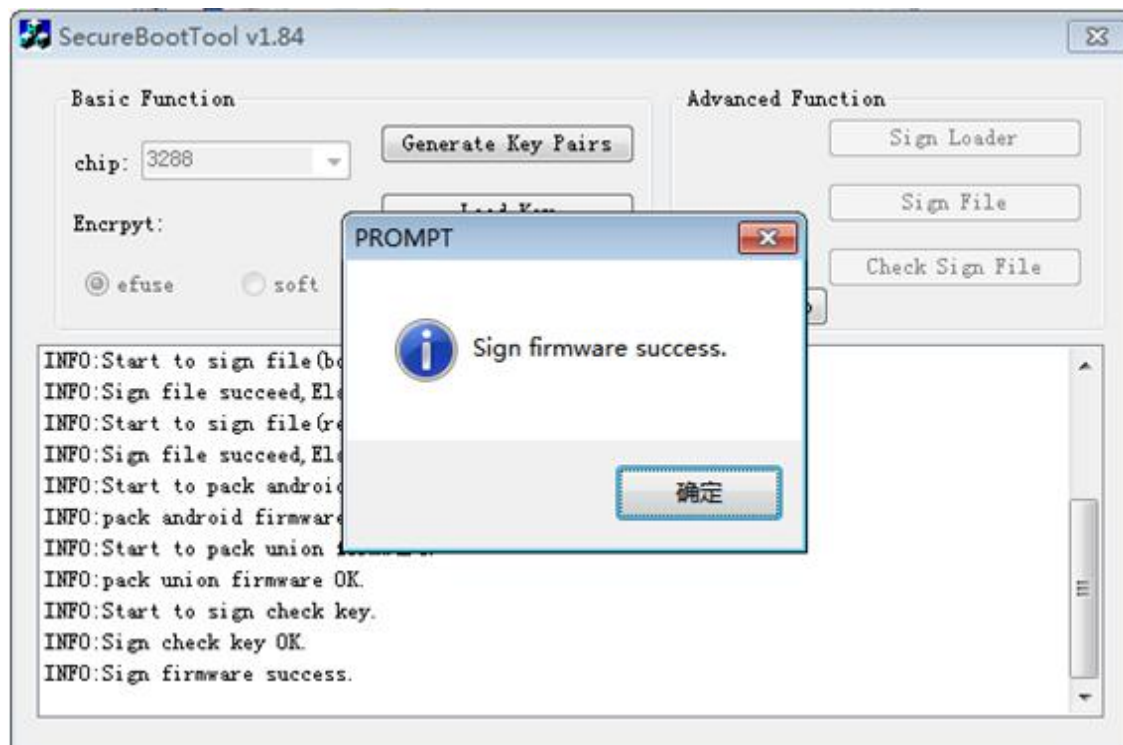


Figure 3-5 SecureBootTool 签名固件

4. 烧写 Efuse

4.1 工具界面

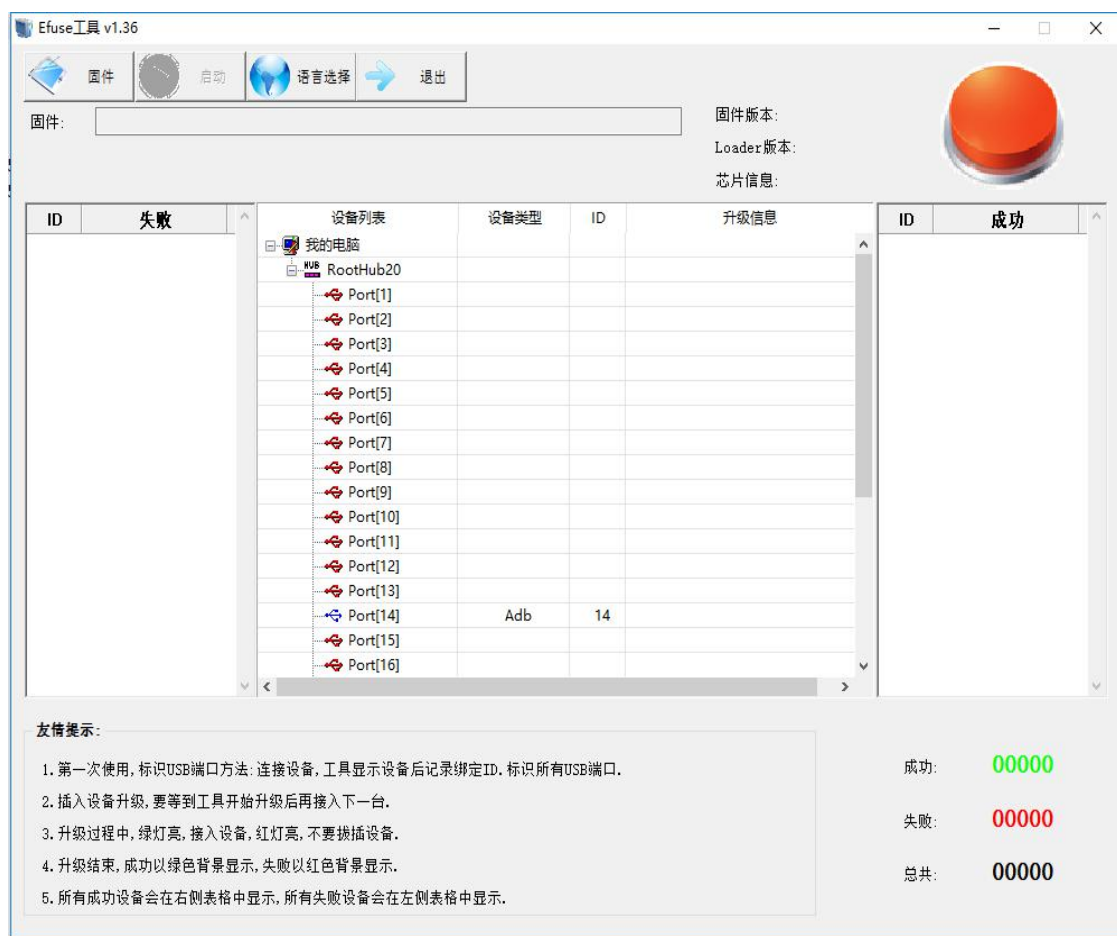


Figure 4-1 EFuse 工具界面

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。

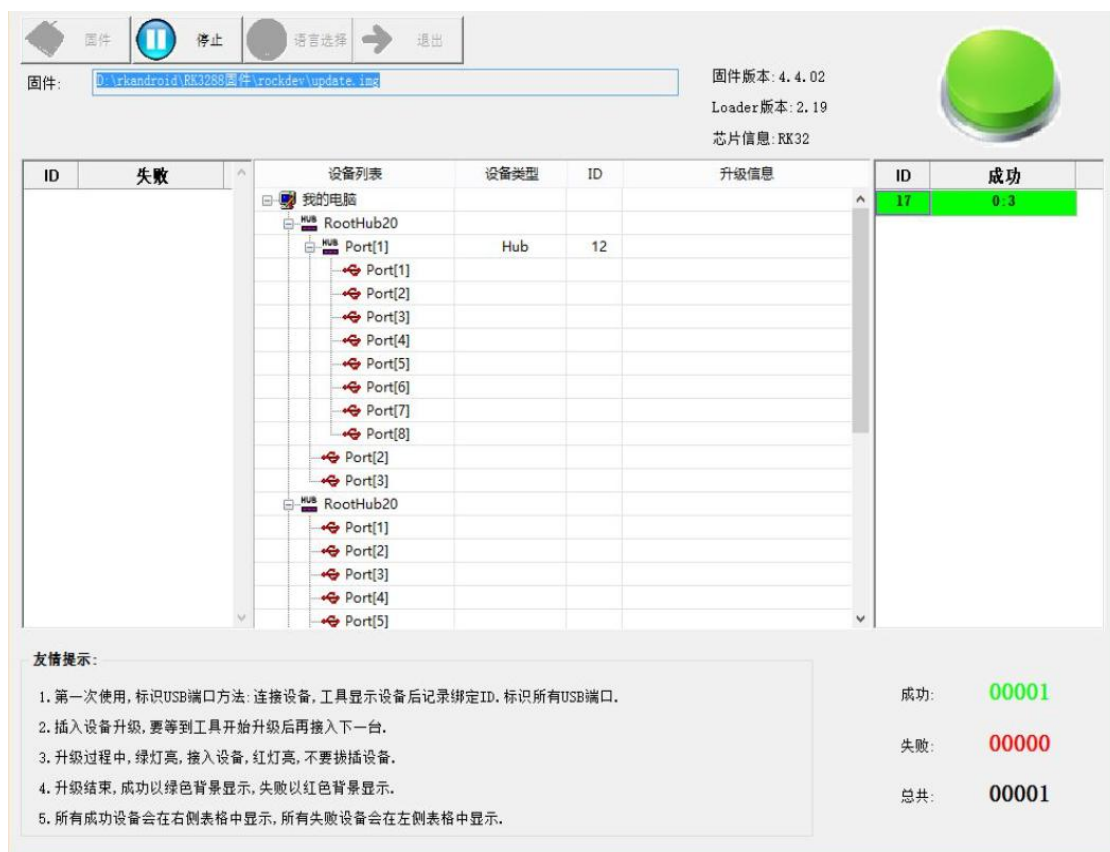


Figure 4-2 FactoryTool 烧写成功

注意事项:

- 1、RK312X、RK3368 需要使用治具，EFUSE 需要单独供电才能烧录；
- 2、RK3288 PCBA 上 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：

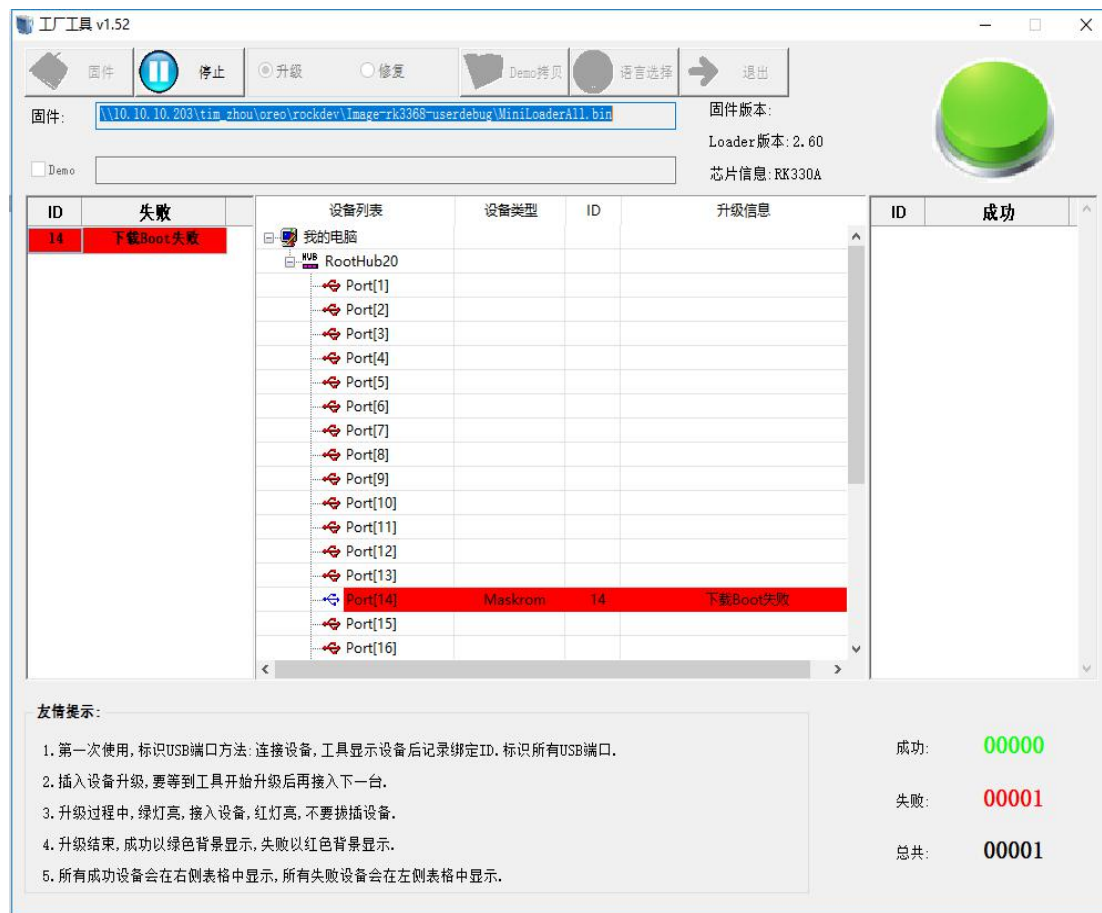


Figure 5-1 工厂工具烧写未签名的固件失败

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；