s-boot场景测试分析

s-boot针对的场景包括只有内部NorFlash和包含外部ROM的情况，同时也要支持程序运行在NorFlash和RAM的情况。针对这些应用需求的场景组合，可以大致列出很多种不同的应用硬件形态。

# 1.基本概念

为了后面的描述方便，这里先定义几个概念如下：

（1）主程序区：就是bootloader优先加载的程序，该区域如果定义在外部区域或者与运行程序区不重合时是加密状态，如果与运行程序区重合，则是解密状态。

（2）备份程序区：这部分程序是在主程序区的代码更新时保留的主程序区的备份。这部分程序只在主程序区的程序可能存在无法升级的BUG或者毁坏时，用于恢复主程序和运行程序所用。这部分是否加密与主程序区是一致的。

（3）运行程序：这部分是程序直接运行的区域，一般程序可以在RAM和内部的NorFlash中运行，这部分程序是解密状态的代码。如果实在RAM中，则一般在启动时从主程序区加载。如果是在NorFlash中，则可以直接从该区域起始位置运行。

（4）加密与解密状态：取决于区域代码包含了img文件头部信息，如果有img文件头部信息，则是加密状态，否则是解密状态。加密状态的代码只有经过解密（如果img文件加密过）并且去掉img文件头部信息后才是可执行的代码，也就是解密状态的代码。

（5）运行ROM：目前已知的只有NorFlash是可以程序随机访问的，也就是可以直接运行程序的ROM。

（6）非运行ROM：大多数的ROM应该是这种，就是只能提供按块访问的存储空间，这种不可以直接运行程序。

（7）系统程序：被bootloader加载和引导的对象，可以是操作系统或者是裸机程序。

# 2.硬件形态分析

目前已知运行ROM（NorFlash）的价格一般远高于非运行ROM，所以一般的硬件上如果同时包含非运行ROM和运行ROM，则前者的空间往往要大得多。基于这个原因，我们约定如果非运行ROM，那么主程序区和备份程序区一定定位在非运行ROM上。这样整个bootloader的形态可以划分为以下的5种。

（1）只有运行ROM，程序运行在运行ROM中，并且运行程序区域主程序区重合。

（2）只有运行ROM，程序运行在运行ROM中，并且运行程序区域主程序区不重合。

（3）只有运行ROM，程序运行在RAM。

（4）有非运行ROM，并且程序运行在运行ROM中。

（5）有非运行ROM，并且程序运行在RAM中。

如果进一步划分，还可以划分更多的子形态。但这五种基本上可以确定所有的程序区的加解密和加载方式。一般外部的ROM是不能直接运行程序的，这样可以确定只有（1）的主程序区和备份程序区是解密状态，其他都是加密状态。

# 3.应用测试场景分析

针对每种不同的硬件形态，每种又包含多种测试用例，部分测试用例还可能有多重应用场景：

3.1下载代码到RAM中直接运行

（1）下载代码到程序缓存中；

（2）校验和解密代码，并去掉img头部；

（3）拷贝代码到运行RAM区域；

（4）引导系统程序到RAM中运行；

3.2下载代码到ROM中

（1）下载代码到程序缓存中；

（2）校验文件img头部，确保完整性；

（3）备份主程序区代码到备份程序区；

（3）根据硬件形态决定是否解密并拷贝代码到主程序区；

（4）根据硬件形态决定是否解密并拷贝到运行ROM区；

（5）引导系统程序运行；

（3）升级程序

（1）在系统程序中下载代码到程序缓存中；

（2）重启进入bootloader；

（3）校验文件img头部，确保完整性；

（4）备份主程序区代码到备份程序区；

（5）根据硬件形态决定是否解密并拷贝代码到主程序区；

（6）根据硬件形态决定是否解密并拷贝到运行ROM区；

（7）引导系统程序运行；

（4）回滚程序

（1）bootloader会在进入系统程序前设置回滚标记；

（2）系统程序如果初始化成功则清除回滚标记；

（3）如果初始化失败或者运行中出现不可恢复硬件错误，则设置回滚标记；

（4）bootloader复位时如果检查到回滚标记有效，则启动回滚；

（5）用备份程序区的程序覆盖主程序区和运行ROM，当然，如果必要，则会解密和去 掉img头部信息。

（5）程序区域损坏

a）主程序区损坏

用备份程序覆盖主程序；

b）备份程序区损坏

用主程序覆盖备份程序；

c）运行ROM区损坏。

优先用主程序覆盖，如果主程序同时损坏，则用备份程序覆盖。