## BP10双秘钥方案

BP10芯片支持code双段加密的功能，即算法用户使用一个秘钥，应用代码使用另外一个秘钥，如图1所示。算法用户将算法秘钥和算法密文烧录到芯片中；然后应用用户基于算法用户提供的芯片和SDK包做二次开发，生成应用代码，可以选择对芯片应用代码进行加密。实现了算法代码和应用代码分别使用不同秘钥的功能。实现双加密功能，还需要配合山景公司提供的烧录工具以及相关的上位机工具，本文主要介绍软件工程方面配置以及相关注意事项。



图1 双秘钥示意图

一、Flash双加密的空间

如图1所示，分段加密的区域一（图中阴影部分），flash的0地址到0x70000（最大值），最大支持448K的代码量（step：64K），此区域为算法代码区域。防止IED debug窗口观测到算法code的二进制文件，我们对icache访问做了限制，最大同样为448K，建议使用16K（step：16K），这个功能一旦启用，则这小段代码中只能是执行代码，不能有数据，比如软件中定义的const table表。分段加密区域二为0x70000地址到flash的容量大小为止，此区域定义为应用代码区。应用用户可以选择对此区域进行加密，也可以是明文。

注意：2个区域的边界地址0x70000不是绝对固定的，是最大值，可以根据工程的需要动态配置烧录。

二、算法工程

算法工程见Demo\_Encryption\_A工程，具体配置详见具体工程，工程支持库形式文件调用，如何添加库文件具体见《AndeSight使用指南.pdf》。如果是调用库文件，则需要在工程中main.c文件中的API调用到库文件中的某一个API，一个c文件中调用一个API即可。工程编译之后需要检查目标API函数是否已经被成功编译到bin文件中，请检查一下 symbol.txt，或者直接查看export.txt文件。

Demo\_Encryption\_A工程编译之后，需要关注编译生成的bin文件大小以及全局变量区域大小，code bin文件的大小（图2暗红色部分，或者看bin文件实际大小）是否会超过工程中的sag文件配置的code size大小，如果大于算法区域的最大值（0x70000），则需要对工程代码重新进行调整，将一部分代码以明文形式放入应用工程。

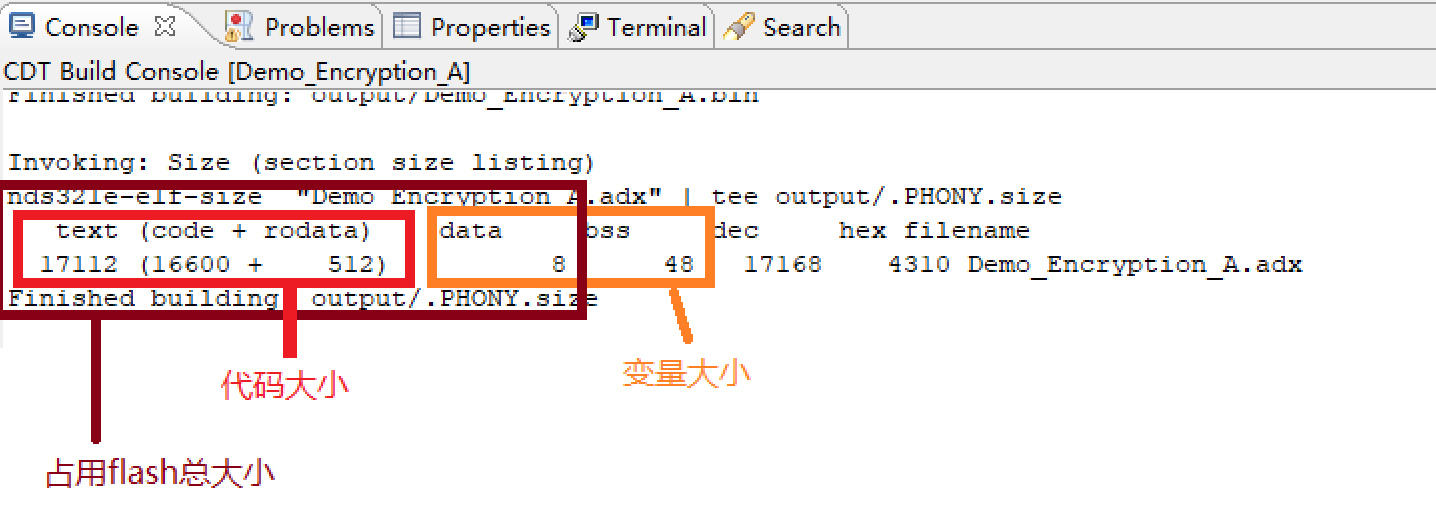


图2 算法工程编译结果

工程编译之后会生成一个export.txt文件，这个文件需要拷贝到Demo\_Encryption\_B。

注意：工程编译之后，data + bss为0，即工程中无全局变量使用，则expert.txt中删除一行：\_SDA\_BASE\_ = 0x20004018; /\* Demo\_Encryption\_A.adx \*/（具体数值不同工程会有所不同），否则应用代码工程编译会出错。

三、应用工程

应用工程山景公司demo见Demo\_Encryption\_B工程。应用代码的demo工程需要算法公司根据山景提供的demo进行修改，本文主要说明工程配置注意事项。

1. 修改sag文件

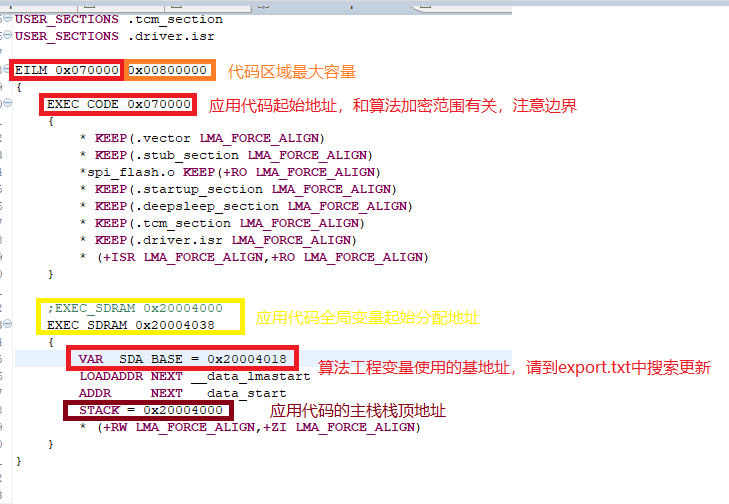


图3 应用工程sag文件配置 1

确认应用工程代码的起始地址是否正确。一般为0x70000，这个地址需要算法工程配置一致，以及算法公司烧录IC的地址，三者均要一致。

确认全局变量起始地址是否正确。

算法工程有全局变量，则计算data + bss总大小，如demo工程编译之后是8 + 48 = 56，转换为16进制为0x38；故应用工程中的sag文件中全局变量起始地址为0x0x20004038 （EXEC SDRAM 0x0x20004038）

算法工程无全局变量，应用工程起始地址则为0x20004000，并且删除VAR SDA\_BASE = 0x20004018；

1. 修改ld文件

如图4红色框内，添加一行代码“INCLUDE "..\export.txt"”，否则算法工程中的函数和变量不能被应用工程调用。

只有当seg文件有更新的时候ld文件才会同步更新，此时才需要添加这行代码。

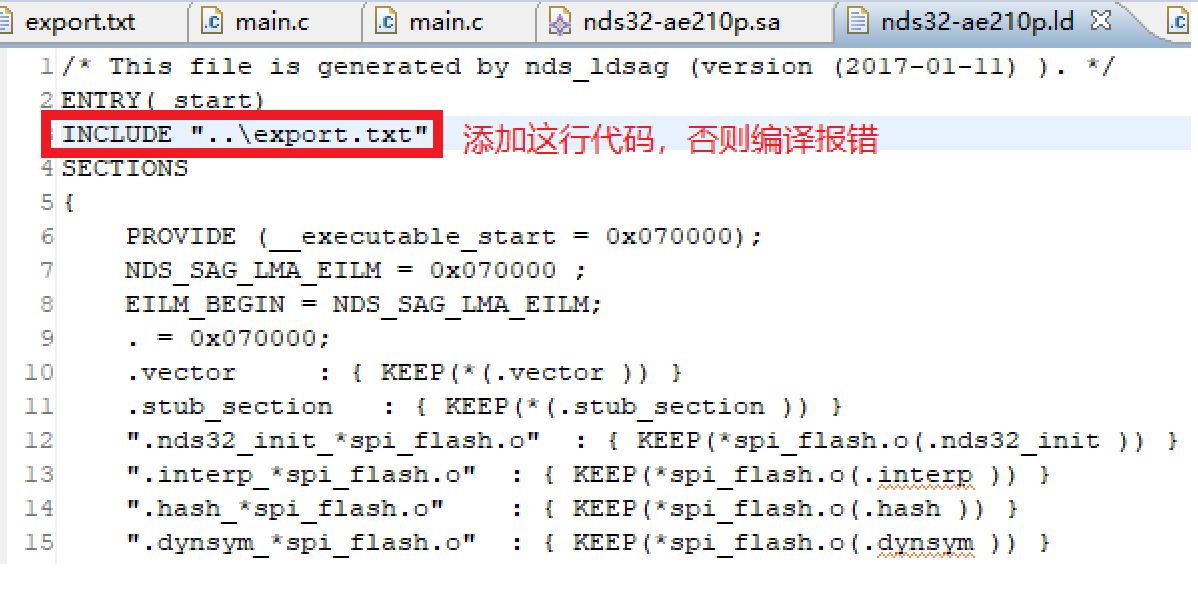


图4 应用工程ld文件配置

1. 应用代码修改

main.c中修改TCM拷贝的起始地址，一般为应用工程代码的起始地址，注意64K对齐。如果算法工程有全局变量，则调用\_\_c\_init\_rom();对算法工程全局变量区域进行处化。

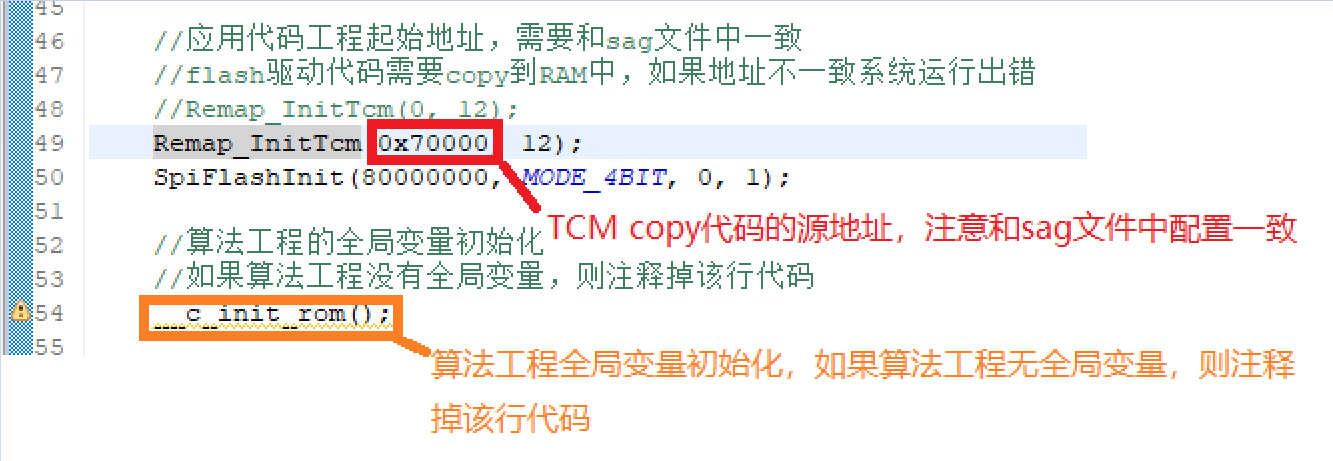


图5 main.c文件修改注意事项

Init\_default.c，修改中断向量表起始地址，为应用代码的起始地址，注意64K对齐。

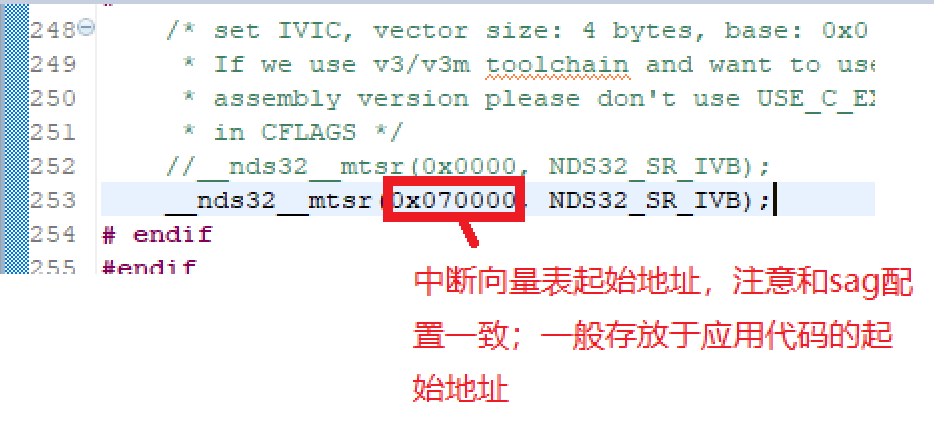


图6 init\_default.c中断向量表配置