

BP15 系列双 key 方案开发说明文档

V0.1

版本记录

版本	日期	修改日志
V0.1	2024-4-30	初版发布

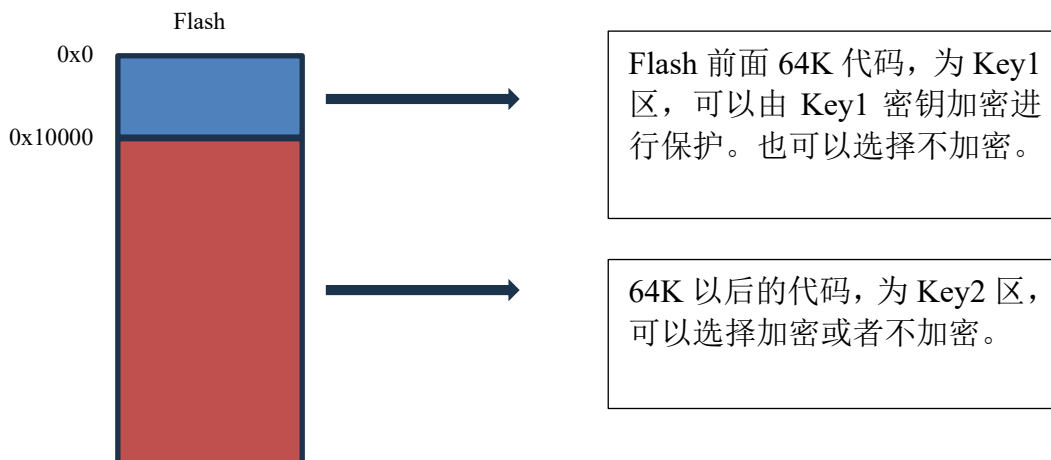
目录

BP15 系列双 key 方案开发说明文档	1
版本记录	1
1 双 key 方案简介	3
2 系统框架	3
2.1 Component_Algorithm	3
2.2 AudioAlgLib	4
2.3 BT_Audio_APP	4
3 下载和调试	5

1 双 key 方案简介

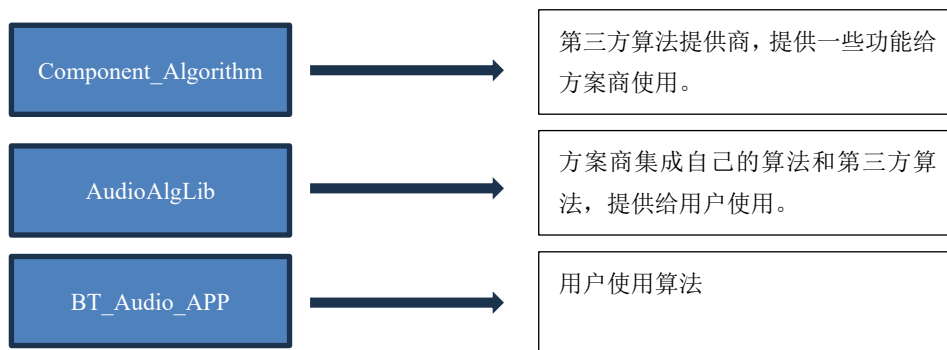
双 key 方案通常是指 Flash 中存放的代码，使用两个密钥来加密和解密数据的一种加密机制，这种机制主要用来保护三方合作的过程中每一方的算法或者代码不被泄漏。

如下图所示，Flash 中分成 2 个区域分别使用 2 个独立的 key 来进行加密。其中第一片区域固定为 64K（0x0~0x10000）。



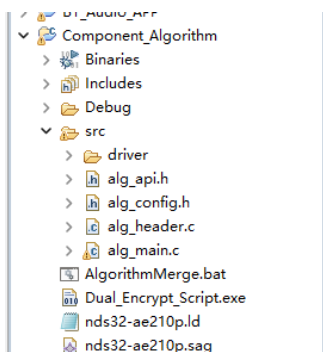
2 系统框架

双 key 方案通常涉及多方合作，每一个合作方都独立管理自己的工程和代码。BP15 SDK 包含了完整的 demo 供参考和使用。



2.1 Component_Algorithm

Component_Algorithm 是 Key1 算法区工程，其中包含 Key1 算法区的结构设置和授权代码示例。工程位于 Examples\examples\Component_Algorithm



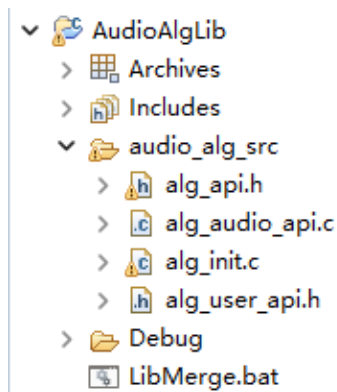
打开 Component_Algorithm 工程,通过 alg_main.c 中的授权示例代码进行授权方案的开发。授权代码开发完成后进行编译,则会生成算法固件(.bin 文件)。output 文件夹中的 Component_Algorithm.bin 是工程编译生成的原始文件,DualAlgorithm_File.bin 文件是通过脚本工具在原始文件的基础上进行相关处理生成。

名称	修改日期	类型	大小
output	2024/4/23 15:45	文件夹	
src	2024/4/22 15:31	文件夹	
Component_Algorithm.adx	2024/4/22 15:31	ADX 文件	567 KB
DualAlgorithm_File.bin	2024/4/22 15:31	BIN 文件	64 KB

- 使用 DualAlgorithm_File.bin 文件进行加密（也可以不加密），烧录到芯片 flash 前面 64K。
- 提供 alg_api.h, 给到方案商使用。

2.2 AudioAlgLib

AudioAlgLib 是音效算法库的示例工程，其中包含通过函数指针的方式将 Key1 算法区的授权函数进行加壳以及认证方案的代码示例。工程位于 Examples\examples\AudioAlgLib



打开 AudioAlgLib 工程，通过 alg_init.c 中的认证示例代码进行认证方案的开发。开发完成后编译代码，会生成库文件（.a 文件），同时会调用脚本 LibMerge.bat 将生成的 Lib 文件以及对于的头文件拷贝至 BT_Audio_APP 工程对应的路径下面，以便于调试。

audio_alg_src	2024/4/22 15:32	文件夹	
output	2024/4/22 15:32	文件夹	
libAudioAlgLib.a	2024/4/22 15:32	A 文件	73 KB
makefile	2024/4/22 15:31	文件	4 KB
objects.mk	2024/4/18 16:13	MK 文件	1 KB
sources.mk	2024/4/22 15:31	MK 文件	1 KB

- 提供 libAudioAlgLib.a 给到客户 BT_Audio_APP 使用。
- 提供 API 使用头文件 alg_user_api.h。

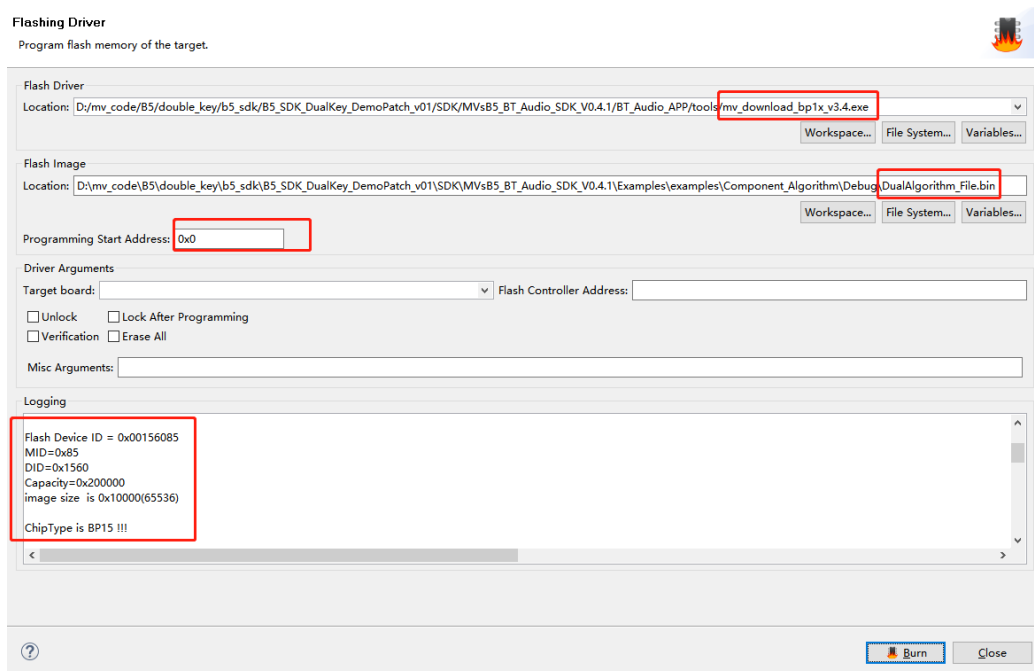
2.3 BT_Audio_APP

BT_Audio_APP 是客户最终的工程，通过头文件和库的方式调用对应的 API。

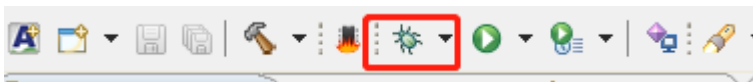
- 打开工程，导入 libAudioAlgLib.a 库和头文件 alg_user_api.h。
SDK 默认已经导入，文件目录在 BT_Audio_APP\app_src\components\algorithm；测试代码在 alg_process.c
- SDK 开启双 key 配置
app_config.h 打卡配置宏 CFG_DOUBLE_KEY_EN

3 下载和调试

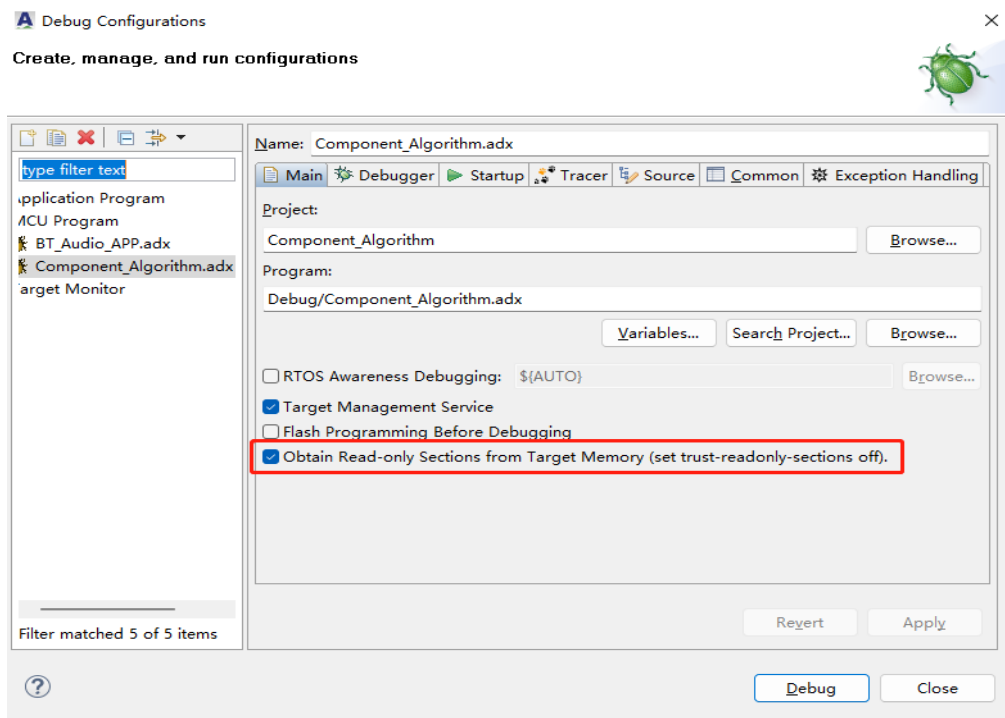
Key1 算法区和 code 单独下载，其中下载 DualAlgorithm_File.bin 文件时的偏移地址是 0x0。而下载 code 则直接下载生成的 MVA 文件即可，若是下载 bin 文件则需要将偏移地址改为 0x10000。Download 使用最新的 bp1x_download_v3.4.exe 下载，其下载工程中的打印信息中包含芯片信息及芯片是否 Key1 加密，可以留意：

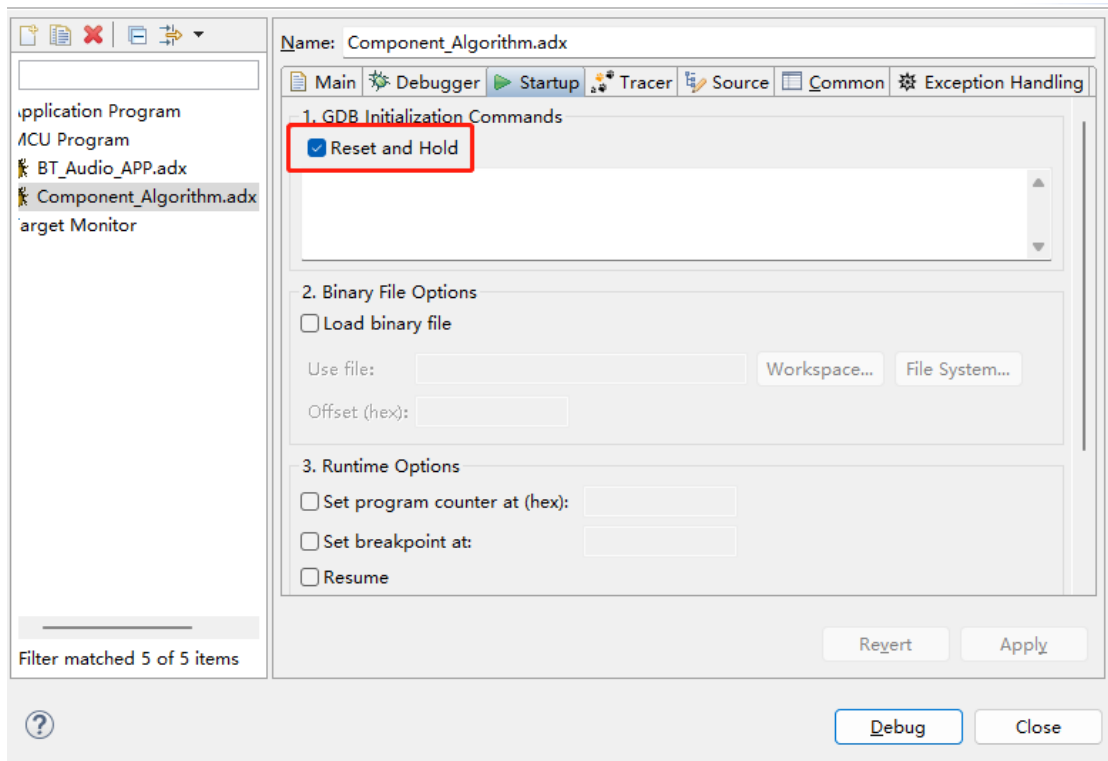


Key1 算法固件和 code 可以独立仿真，在对应工程下面点击仿真图标进行仿真。

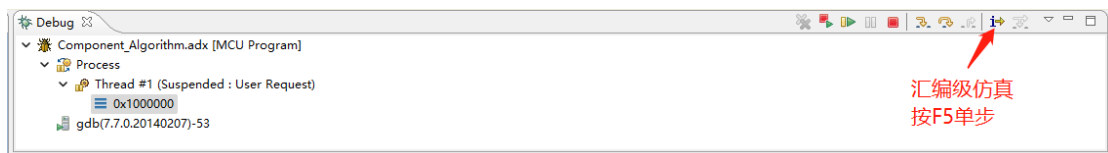


仿真通常的设置如下：

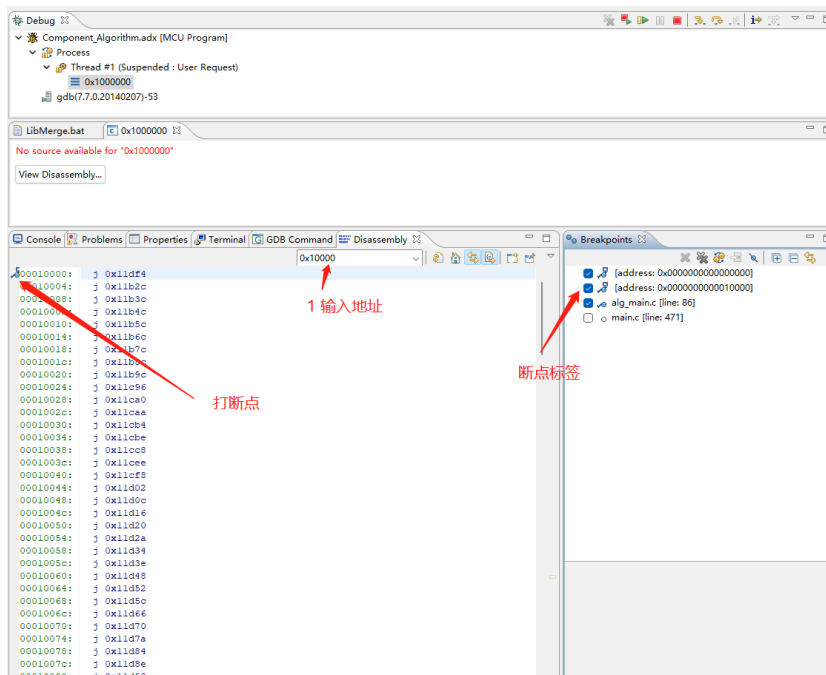




注意，如下图所示图标为汇编级单步，有需要可以使用：



可以配合汇编级断点俩进一步调试：



注：如果 Key1 区域加密之后，这段区域会被保护，仿真时是拿不到反汇编的。同时如果 code 被加密则无法进行仿真。因此需要在未加密状态下进行调试。