ACM32F403/FP401/A403/F0X0/A070/WB15
存储保护功能使用方法

介绍

本文档将介绍 ACM32F403/FP401/A403/F0X0/A070/WB15 系列芯片存储保护功能的使用方法。

本系列芯片的存储保护功能有以下类型：

WRP（Write Protection）写保护：防止意外的对存储器的擦、写操作。

PCROP（Proprietary code read out protection）专有代码读保护：针对指定区域进行读写保护。

1. 用于存储保护的 NVR 寄存器

芯片 EFLASH 的 NVR 区域有一些专用于存储保护的寄存器（32bit 位宽）。

NVR 起始地址：0x00080000

如需了解 NVR 寄存器的详细信息，请联系公司 FAE。

用户代码中对 NVR 区域寄存器的修改，需要读出整页，修改寄存器对应偏移地址数据，再擦除和编程该页。

1.1. NVR4 只读保护

用户在设置 WRP 使能或 PCROP 使能后，建议将 NVR4 页设置为只读属性。否则下载工具或用户代码可以禁止 WRP 或 PCROP。

通过下载工具或用户代码对 OTP4_EN 寄存器写入 0x55aa77ee（复位后生效），就可开启 NVR4 页的只读保护。

1.2. EFC 复位

复位控制寄存器（0x40010800，系统寄存器区域）的 EFC_RST 位（bit29）置 0，芯片复位并发起 NVR 重新加载，复位层级和 NRST 复位相当。

2. WRP 写保护

WRP 被用来保护特定扇区（以 2KB 为单位）的内容，防止代码被擦除或重写。

写保护可以通过下载工具或者在用户代码中使能。

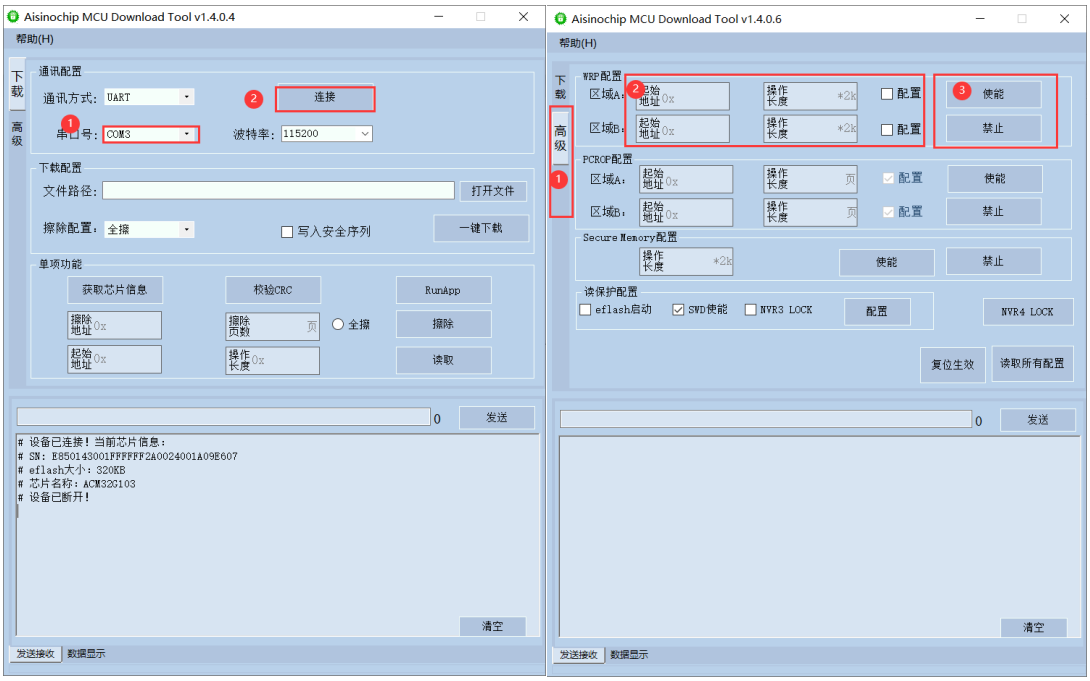
2.1. 通过下载工具使能或禁止 WRP

首先连接目标芯片。

切换到“高级”页面，配置区域的地址和长度，点击“使能”或“禁止”按钮。

选中“NVR4 LOCK”复选框，点击旁边的“配置”按钮，将 NVR4 页设置为只读属性。

RSTN/POR /EFC 复位重启后生效。



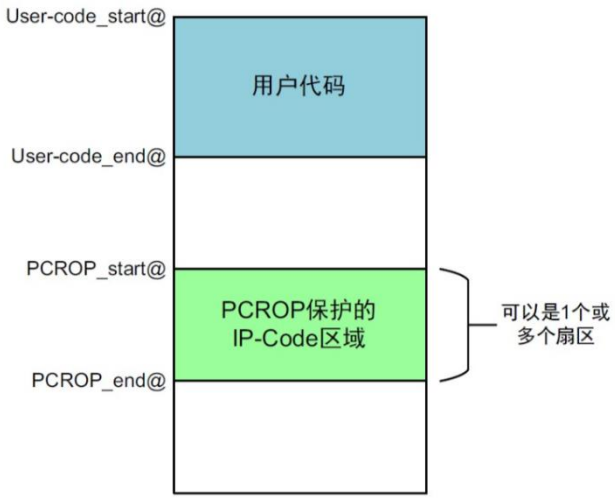
2.2. 用户代码中使能或禁止 WRP

用户代码中，对 NVR 区域的 WRP_EN、WRP_AREA_A、WRP_AREA_B 寄存器进行配置。再对 OTP4_EN 寄存器进行配置，使能 NVR4 只读保护。

RSTN/POR /EFC 复位重启后生效。

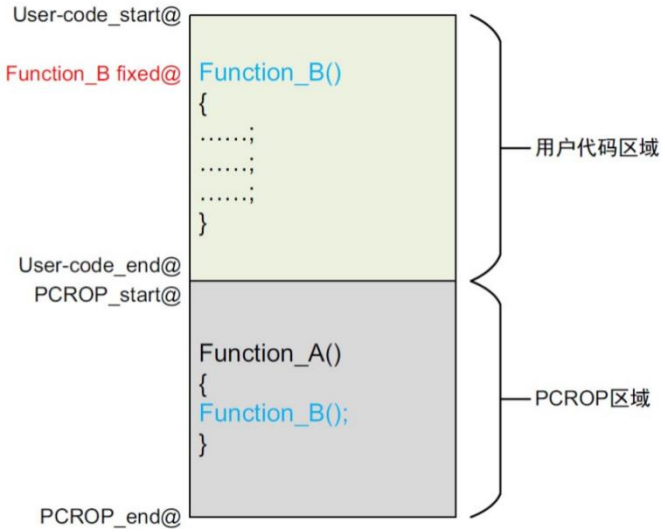
3. PCROP 专有代码读保护

PCROP 是一个专有代码读出保护的功能。它是针对 Flash 的某些特定区域进行代码的读写保护。可以被用来保护一些 IP 代码，方便进行二次开发。



受 PCROP 保护的 IP 代码可以随意地被用户应用程序调用运行，同时又防止外界对 IP 代码的直接读写访问。

PCROP 区的代码也可以调用 PCROP 区外的处于固定地址的函数。



受 PCROP 保护的区域中只允许执行指令代码（通过 I-Code 总线取指令），数据读取是被禁止的。因此，受保护的 IP 代码不能访问存储于同一块区域内的关联数据，比如文字池（literal pools）、分支表（branch tables）以及在执行过程中需要通过 D-code 总线进行读取的常量数据。

换言之，受 PCROP 保护的代码只能是只执行的指令代码，而不包含任何数据。因此，我们在编译受 PCROP 保护的 IP 代码时，必须对其进行相应配置，以避免在 PRROP 区域生成文字池、常量数据等。

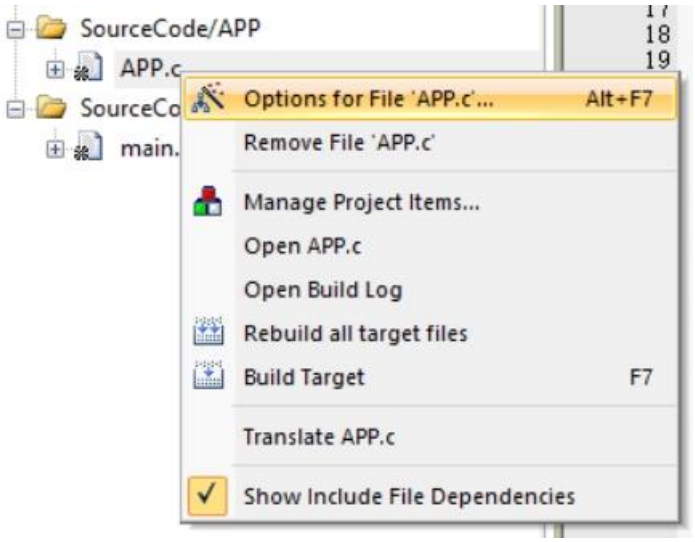
以下为示例说明：例如，假设您指定 0x10000-0x13000 为 PCROP 保护区域，则不能在该地址范围中定义常量数据。（exp: const uint32_t val __attribute__((at(0x00010000))) =

0x12345678，类似这样的操作是不允许的）。

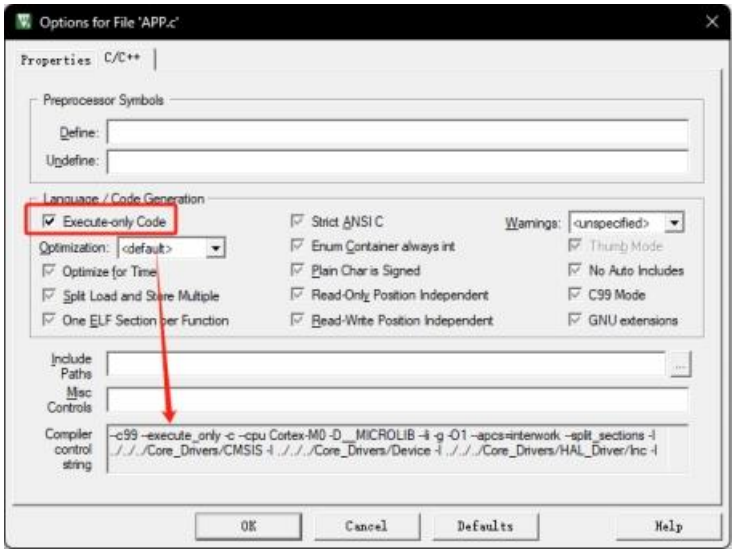
MCU 的中断向量表里都是些常量数据，所以包含中断向量表的扇区不可进行 PCROP。一般来讲向量表放在第一个扇区，所以该扇区不可进行 PCROP。

不同的编译工具链有其自己的配置方式去阻止编译器生成文字池和分支表。我们来看一下基于 MDK 中设置操作。

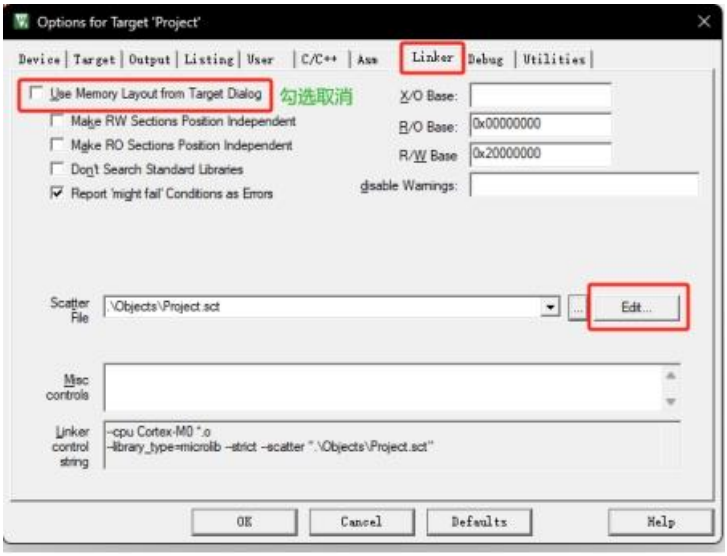
1）右击项目中的需要保护代码文件，选择“Options for File‘APP.c’”

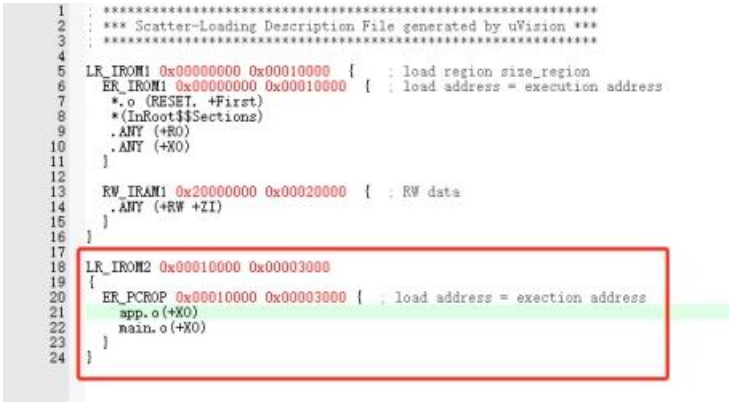


2）在对话框中选择“C/C++”页面，选中“Execute-only Code”，点“OK”



3）修改 scatter file（.sct 文件），设置 APP 代码为只可执行代码：





示例代码如下：

```
LR_IROM1 0x00000000 0x00010000  {    ; load region size_region
  ER_IROM1 0x00000000 0x00010000  {  ; load address = execution address
   *.o (RESET, +First)
   *(InRoot$$Sections)
   .ANY (+RO)
   .ANY (+XO)
  }
  RW_IRAM1 0x20000000 0x00030000  {  ; RW data
   .ANY (+RW +ZI)
  }
}

; code protect section
LR_IROM2 0x00010000 0x00003000
{
    ER_PCROP 0x00010000 0x00003000 {
        app.o (+XO)
        main.o (+XO)
```

```
        }
    }
```

如上图所示，修改工程中的.sct 分散加载文件，原本 sct 文件只有 LR_IROM1 这一块区域，总大小为 0x80000(512K)，修改后区域被划分为 LR_IROM1（0x00000-0x10000）和 LR_IROM2（0x10000-0x13000）,其中 LR_IROM2 区域用于设置 PCROP 保护功能存放需要读保护的目代码，例程中假设 main.c 和 app.c 是需要保护的源码文件，故将其编译后生成的 app.o 和 main.o 文件放入加密区域 LR_IROM2 中的 ER_PCROP，并加上(+XO)后缀，表示代码是 Execute-only 的。（记得先按第一步中的操作勾选 Execute-only Code）

PCROP 保护可以通过下载工具或者在用户代码中使能。

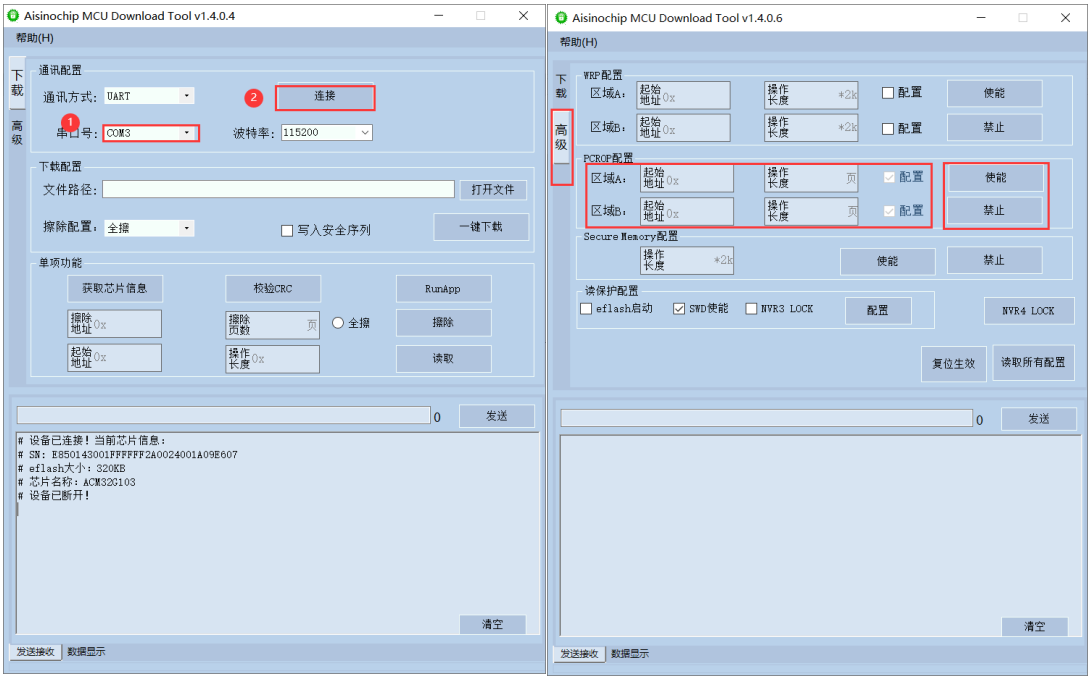
3.1. 通过下载工具使能或禁止 PCROP

首先连接目标芯片。

切换到“高级”页面，配置区域的地址和长度（长度以 512 字节为单位），点击“使能”或“禁止”按钮。

点击“NVR4 LOCK”按钮，将 NVR4 页设置为只读属性。（可选）

RSTN/POR /EFC 复位重启后生效。



PCROP 使能时，必须同时对两个区域进行配置，区域不得超出 FLASH 范围。如果只希望保护一个区域，则另一个区域操作起始地址设置为 0xFFFF，长度设为 0，PC 工具会对寄存器写入 0x0000FFFF，表示该区域保护禁止。

PCROP 禁止时，需要将 SWD 使能关闭，复位或重新上电方能生效。

3.2. 用户代码中使能或禁止 PCROP

用户代码中，对 NVR 区域的 PCROP_EN、PCROP_AREA_A、PCROP_AREA_B、OTP4_EN 寄存器进行配置。

在 PCROP_EN 使能前，务必同时对 PCROP_AREA_A、PCROP_AREA_B 进行设置，不得超出 FLASH 范围。如果只希望保护一个区域，则另一个区域可设置为 0x0000FFFF，表示该区域保护禁止。

再对 OTP4_EN 寄存器进行配置，使能 NVR4 只读保护。（可选）

RSTN/POR /EFC 复位重启后生效。

如果 NVR4 只读保护使能，则无法直接禁止 PCROP，只能发起降级流程。

3.3. PCROP 降级

NVR4 只读保护使能后，不能通过写 NVR4 寄存器来禁止 PCROP，只能通过降级流程操作。

PCROP 降级会擦除 PCROP 区域代码。

操作步骤：

1）擦除安全启动序列

如果用户之前在 NVR3 区域 BOOT_PATTEN 寄存器写过安全启动序列，且希望降级后通过下载工具下载新的代码，则在降级前需要擦除安全启动序列。

如果是通过 JTAG 下载新的代码，则不需擦除安全启动序列。

2）使用 EFLASH 操作接口对 NVR3 区域寄存器进行如下操作：

PCROP_ DEGRADE1 寄存器按写入：0xFFFC0003：A/B 区降级；

PCROP_ DEGRADE2 寄存器写 0x89BC3F51；

JTAG_DISABLE 寄存器写 0x89BC3F51。

3）RSTN/POR /EFC 复位

EFC 复位方法，参见 1.2 节。

复位重启后，芯片会执行降级操作：将 PCROP 功能禁止，并擦除被保护代码（页擦，空间较大时，时间较长）、擦除 OTP4_EN 标志、使能 JTAG、执行 EFC 复位。

降级完成标志为：PCROP_ DEGRADE1 寄存器读出的数据不再是高低 16 位取反。

联系我们

公司：上海航芯电子科技股份有限公司
地址：上海市闵行区合川路 2570 号科技绿洲三期 2 号楼 702 室
邮编：200241
电话：+86-21-6125 9080
传真：+86-21-6125 9080-830
Email： Service@AisinoChip.com
Website： www.aisinochip.com

版本维护

版本	日期	作者	描述
V1.0	2023-11-7	Aisinochip	初始版