应用笔记

ACM32F403 / A403 / FP401 / F070 / A070 / WB15 系列芯片
存储保护功能

版本：V1.2

日期：2025-3-10

上海航芯电子科技股份有限公司

1. 概述

本文档将介绍 ACM32F403 / A403 / FP401 / F070 / 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。

2. 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

名称	地址偏移	描述	默认值
NVR3			
BOOT_PATTEN	0x400	安全启动序列	not 0x89bc3f51：BOOT 启动(default)； 0x89bc3f51：flash 启动。
JTAG_DISABLE	0x41C	JTAG 禁止	not 0x89bc3f51：JTAG 使能(default)； 0x89bc3f51：JTAG 禁止。
PCROP_ DEGRADE1	0x484	PCROP 降级标志 1	0xFFFC0003：申请 A/B 区同时降级
PCROP_ DEGRADE2	0x488	PCROP 降级标志 2	0x89BC3F51：申请 PCROP 降级操作完成后，擦除 JTAG_DISABLE 和 OTP4_EN 标志
NVR4			
PCROP_EN	0x600	Flash PCROP 保护使能。使能后，PCROP area A/B 只能执行，不能读取或者擦写。	not 0x89bc3f51：PCROP 功能不使能(default)； 0x89bc3f51：PCROP 功能使能
PCROP_AREA_A	0x604	PCROP area A 地址定义，以 page（512 字节）为单位。 [9:0] ： PCROP1A_STRT[9:0] [25:16] ： PCROP1A_END[9:0] Bit[15:10],bit[31:26]写 0。 起始地址 PCROP1A_STRT*0x200（包括） 结束地址(PCROP1A_END+1)*0x200（不包括）	0xFFFFFFFF(default)：保护第 1023 页。(对于 F0 系列，FLASH 只有 256 页， PCROP_EN 使能前，必须修改该值，否则芯片会死机。) 0x0000FFFF：PCROP 保护禁止。
PCROP_AREA_B	0x608	PCROP area B 地址定义，以 page（512 字节）为单位。 [9:0] ： PCROP1B_STRT[9:0] [25:16] ： PCROP1B_END[9:0] Bit[15:10],bit[31:26]写 0。 起始地址 PCROP1B_STRT*0x200（包括） 结束地址(PCROP1B_END+1)*0x200（不包括）	0xFFFFFFFF(default)：保护第 1023 页。(对于 F0 系列，FLASH 只有 256 页， PCROP_EN 使能前，必须修改该值，否则芯片会死机。) 0x0000FFFF：PCROP 保护禁止。
WRP_EN	0x620	Flash WRP 保护使能。使能后，WRP areaA/B 禁止擦写。	not 0x89bc3f51：WRP 功能不使能(default)； 0x89bc3f51：WRP 功能使能

WRP_AREA_A	0x624	WRPP area A 地址定义，以 2K 字节为单位。 [7:0] ： WRP1A_STRT[7:0] [23:16] ： WRP1A_END[7:0] 起始地址 WRP1A_STRT*0x800（包括） 结束地址(WRP1A_END+1)*0x800（不包括）	
WRP_AREA_B	0x628	WRPP area B 地址定义，以 2K 字节为单位。 [7:0] ： WRP1B_STRT[7:0] [23:16] ： WRP1B_END[7:0] 起始地址 WRP1B_STRT*0x800（包括） 结束地址(WRP1B_END+1)*0x800（不包括）	
FUNC_PATCH_EN	0x680		必须为 0x6789a55a，否则不支持 PCROP 功能
FUNC_PATCH1_ADDR	0x684		必须为 0x10080801，否则不支持 PCROP 功能
OTP4_EN	0x7FC	NVR4 区 OTP 使能位。	0x55aa77ee：NVR4 只允许读。 其它值：NVR4 页可以任意访问 (default)

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。

2.1. 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。

2.2. 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。

3. 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。

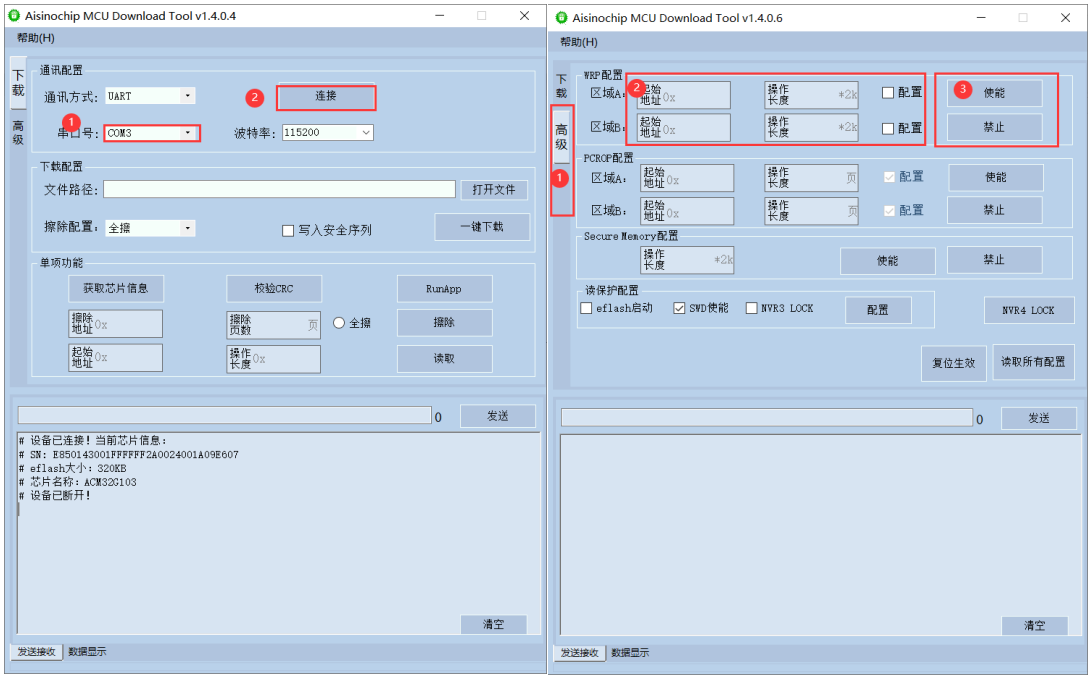
3.1. 通过下载工具使能或禁止 WRP

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。



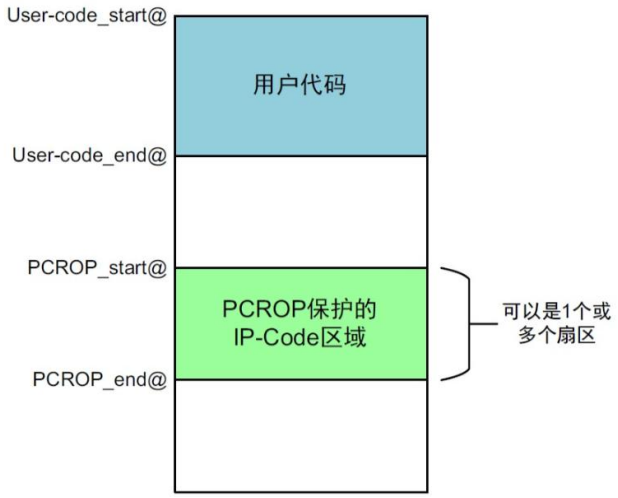
3.2. 用户代码中使能或禁止 WRP

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。

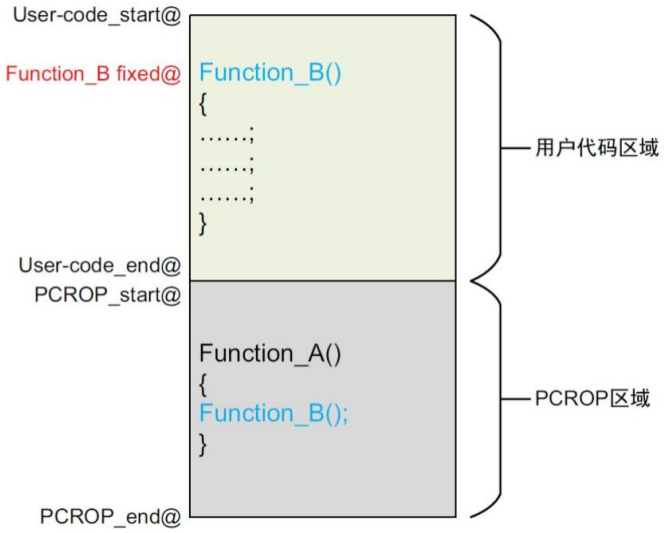
4. PCROP 专有代码读保护

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。



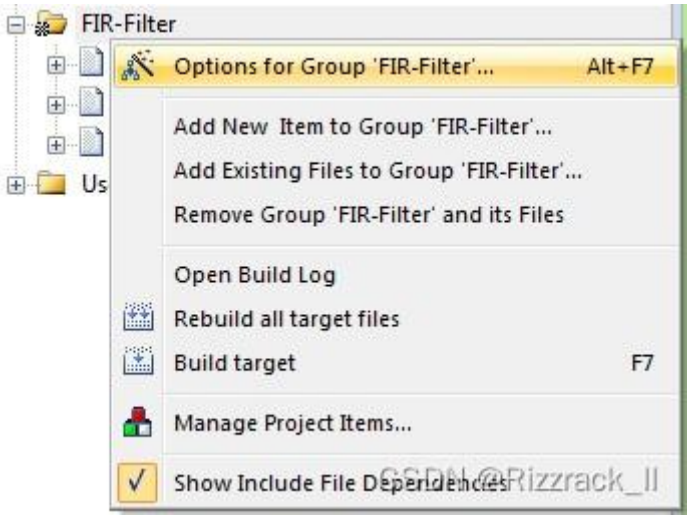
受 PCROP 保护的区域中只允许执行指令代码（通过 I-Code 总线取指令），数据读取是被禁止的。因此，受保护的 IP 代码不能访问存储于同一块区域内的关联数据，比如文字池（literal pools）、分支表（branch tables）以及在执行过程中需要通过 D-code 总线进行读取的常量数据。

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。

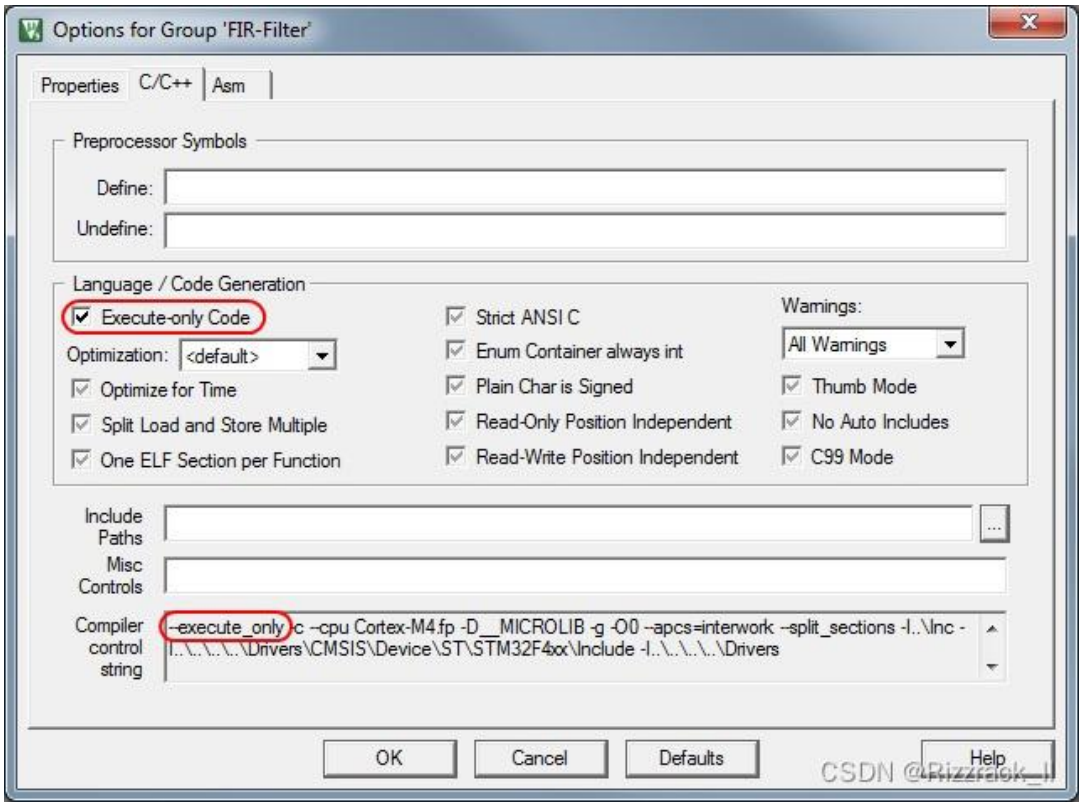
MCU 的中断向量表里都是些常量数据，所以包含中断向量表的扇区不可进行 PCROP。一般来讲向量表放在第一个扇区，所以该扇区不可进行 PCROP。

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 IP 代码文件组，选择“Options for Group‘FIR-Filter’”



在对话框中选择“C/C++”页面，选中“Execute-only code”，点“OK”。



2) 另外，还需修改 scatter file（.sct 文件），设置 IP 代码为只可执行代码：

```
LR_PCROP 0x08008000 0x00004000 {
    ER_PCROP 0x08008000 0x00004000 { ; load address = execution address
        arm_fir_f32.o (+XO)
        arm_fir_init_f32.o (+XO)
        FIR_Filter.o (+XO)
    }
}
```

PCROP 保护可以通过下载工具或者在用户代码中使能。

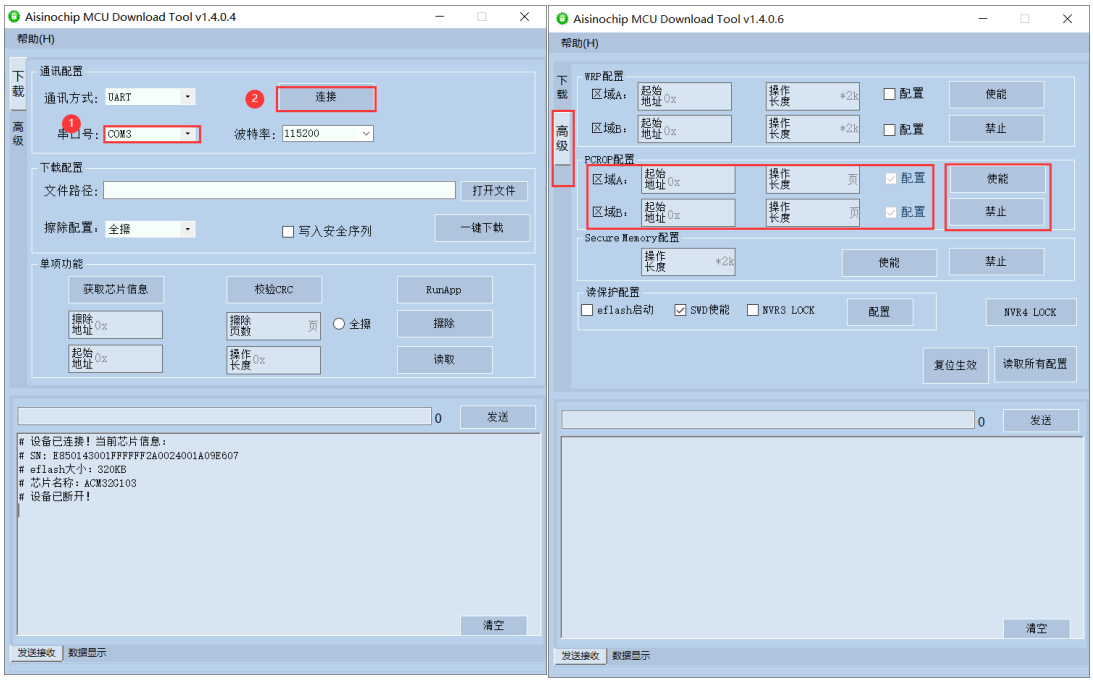
4.1. 通过下载工具使能或禁止 PCROP

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。

4.2. 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。

4.3. 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。

5. 版本历史

版本	日期	作者	描述
V1.0	2021-04-30	Hangxin	初始版
V1.1	2023-02-10	Hangxin	添加 A070 系列芯片支持
V1.2	2025-03-10	Hangxin	添加 WB15 系列芯片支持

6. 版权声明

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@HangChip.com

Website： www.hangChip.com