应用笔记

ACM32G103 系列芯片

存储保护功能

版本：V1.1

日期：2024-6-19

上海航芯电子科技股份有限公司

1. 概述

本文档将介绍 ACM32G103 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：

RDP（Read Protection）读保护：对整个芯片实施读保护。

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			
REMAP	0x400	安全启动序列	not 0x89bc3f51：BOOT 启动(default)； 0x89bc3f51：flash 启动。
PCROP_ DEGRADE	0x484	PCROP 降级标志	0xFFFC0003：申请降级，擦除 PCROP 保护区域 0xFFFB0004：申请降级，擦除全片 EFLASH
RDP1_DEGRADE	0x488	RDP1 降级标志 是否需要 RDP 降级，高低 16 位取反有效	高低 16 位未取反：不需要 RDP 降级(default)； 高低 16 位取反：申请 RDP 降级
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] 起始地址 PCROP1A_STRT*0x200（包括） 结束地址(PCROP1A_END+1)*0x200（不包括）	
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] 起始地址 PCROP1B_STRT*0x200（包括） 结束地址(PCROP1B_END+1)*0x200（不包括）	
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）	
RDP1_EN	0x660	RDP1 使能标志。使能 RDP1 功能后，BOOT 模式和 JTAG 无法读取 Flash 主区内容	not 0x89bc3f51：RDP1 功能不使能(default)； 0x89bc3f51：RDP 功能使能
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

3. RDP 读保护

RDP 读保护是一种全局 FLASH 读保护。可以防止代码拷贝、反向工程、JTAG 读取等攻击。

用户应在固件下载完成后，再使能 RDP 保护。

3.1. RDP L0

L0 级保护是默认的等级，FLASH 是完全开放的，BOOT 模式和 JTAG 模式下可对 FLASH 进行各种读写擦操作。

3.2. RDP L1

当 L1 保护等级激活，BOOT 模式和 JTAG 模式下不可访问 FLASH。但是从 FLASH 启动的用户代码是可以访问 FLASH 的。

当 L1 保护等级激活后，代码的更新不能通过 BOOTLOADER 或 JTAG 进行。但用户代码可以自行设计 IAP 功能来自更新代码。

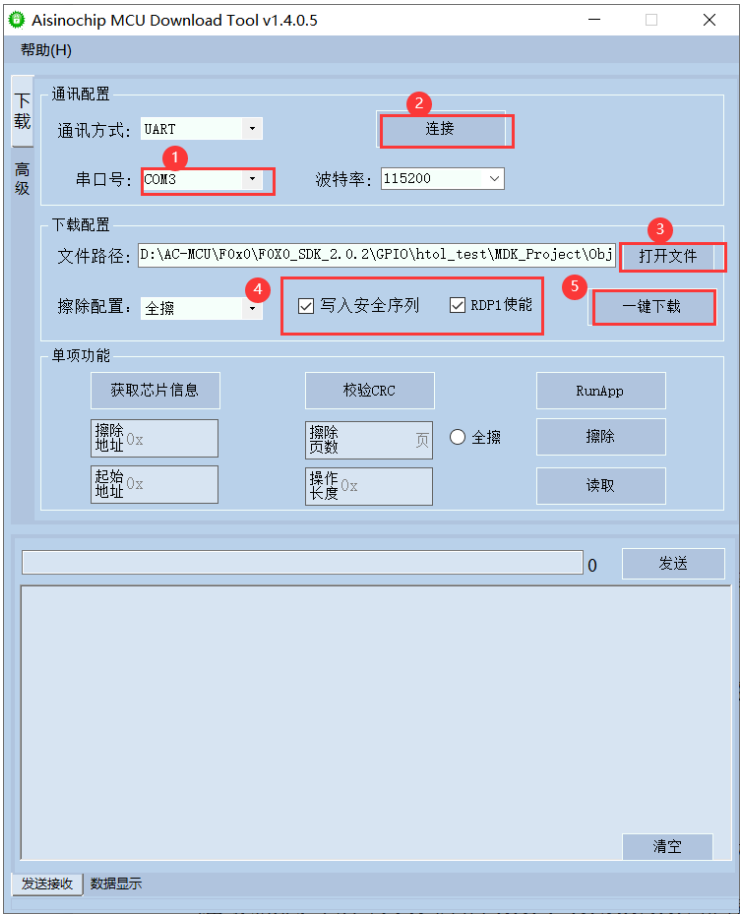
3.3. RDP L1 激活

当芯片处于 L0 保护等级，可以通过下载工具使能 RDP L1，或者在用户代码中使能 RDP L1。

3.3.1. 在下载工具的下载代码流程中使能 RDP1

下载工具的“下载”页面，连接目标芯片，现在需要下载的代码文件，选中“写入安全序列”和“RDP1 使能”复选框，点击“一键下载”按钮。

代码下载完成后，复位或断电重启，配置就生效了。



3.3.2. 用户代码中使能 RDP1

用户代码中，设置 RDP1 使能标志（读取 NVR 区的 RDP1_EN 寄存器，如果不是 0x89bc3f51 的话，则写入 0x89bc3f51）。

3.4. RDP L1 降级

当芯片处于 RDP L1 保护等级，如果用户希望回到 BOOT 模式更新代码，则需要进行 RDP 降级，让芯片回到 RDP L0 等级。

从 L1 降级到 L0 会导致 FLASH 数据全部擦除。

■ 降级步骤：

1）用户代码中设置 RDP1 降级标志。

用户代码中，擦除安全启动序列（对 NVR 区的 REMAP 寄存器写入 0xFFFFFFFF），然后写降级标志（对 NVR 区的 RDP1_DEGRADE 寄存器写入 0x0000FFFF）。

2）复位或断电重启后生效。

复位或断电重启后，芯片 BOOT 代码检测到 RDP1 降级标志，会强制擦除 FLASH 全部数据，擦除 RDP1_EN 寄存器和 RDP1_DEGRADE 寄存器。芯片重新回到 RDP L0 等级。

4. 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。

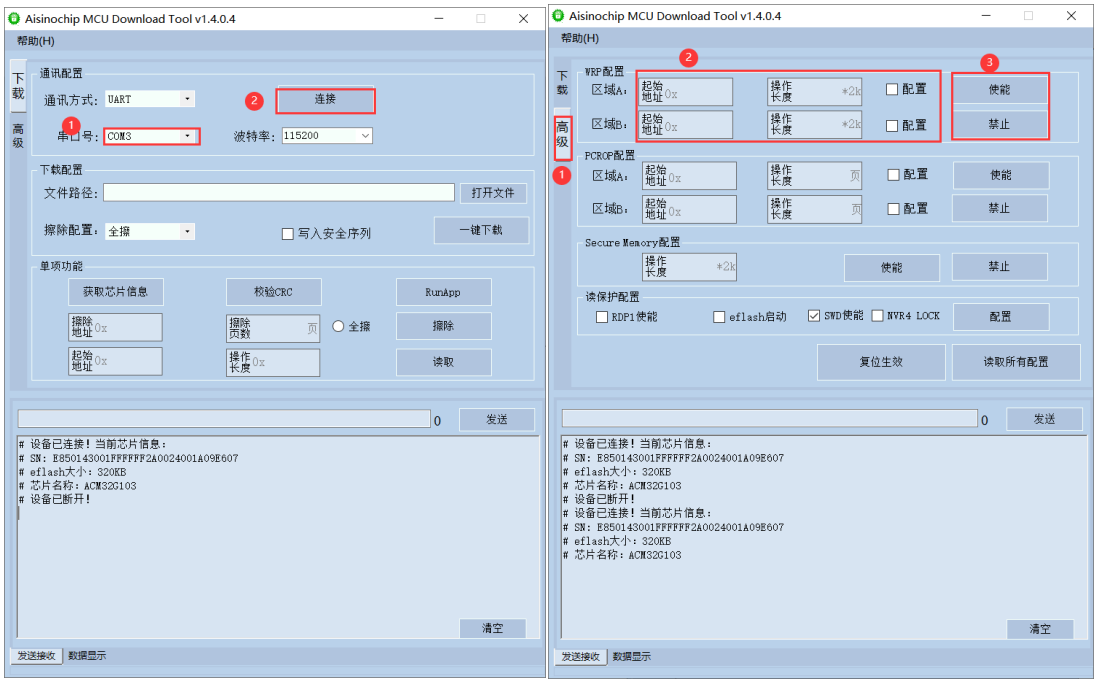
写保护可以通过下载工具或者在用户代码中使能。

4.1. 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。

复位或断电重启后生效。



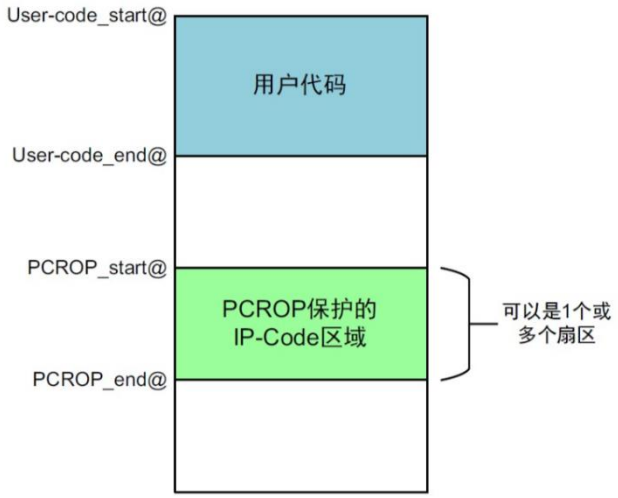
4.2. 用户代码中使能或禁止 WRP

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。

复位或断电重启后生效。

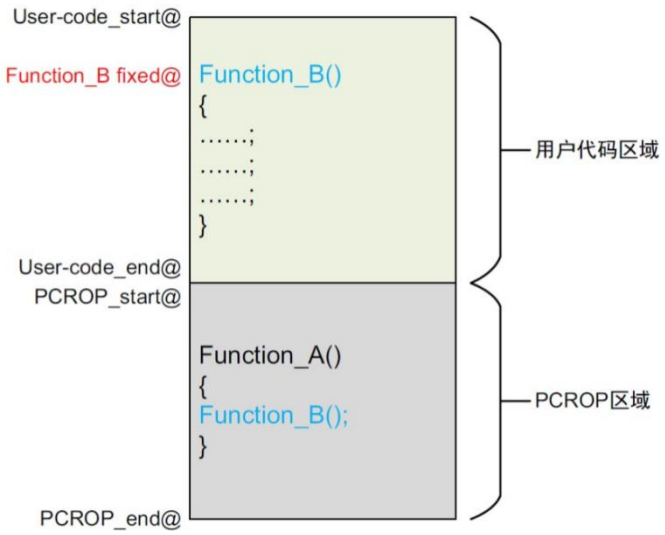
5. PCROP 专有代码读保护

PCROP 是一个专有代码读出保护的功能。与 RDP 对整片 Flash 读保护不同的是，它只是针对 Flash 的某些特定区域进行代码的读写保护。它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。



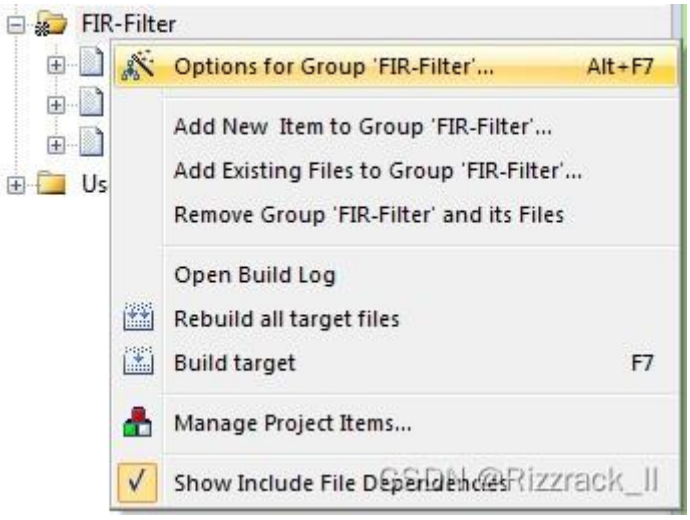
受 PCROP 保护的区域是无法使用 D-Code 总线进行读访问的，所以在这片区域中只允许执行指令代码（通过 I-Code 总线取指令），数据读取是被禁止的。因此，受保护的 IP 代码不能访问存储于同一块区域内的关联数据，比如文字池（literal pools）、分支表（branch tables）以及在执行过程中需要通过 D-code 总线进行读取的常量数据。

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。

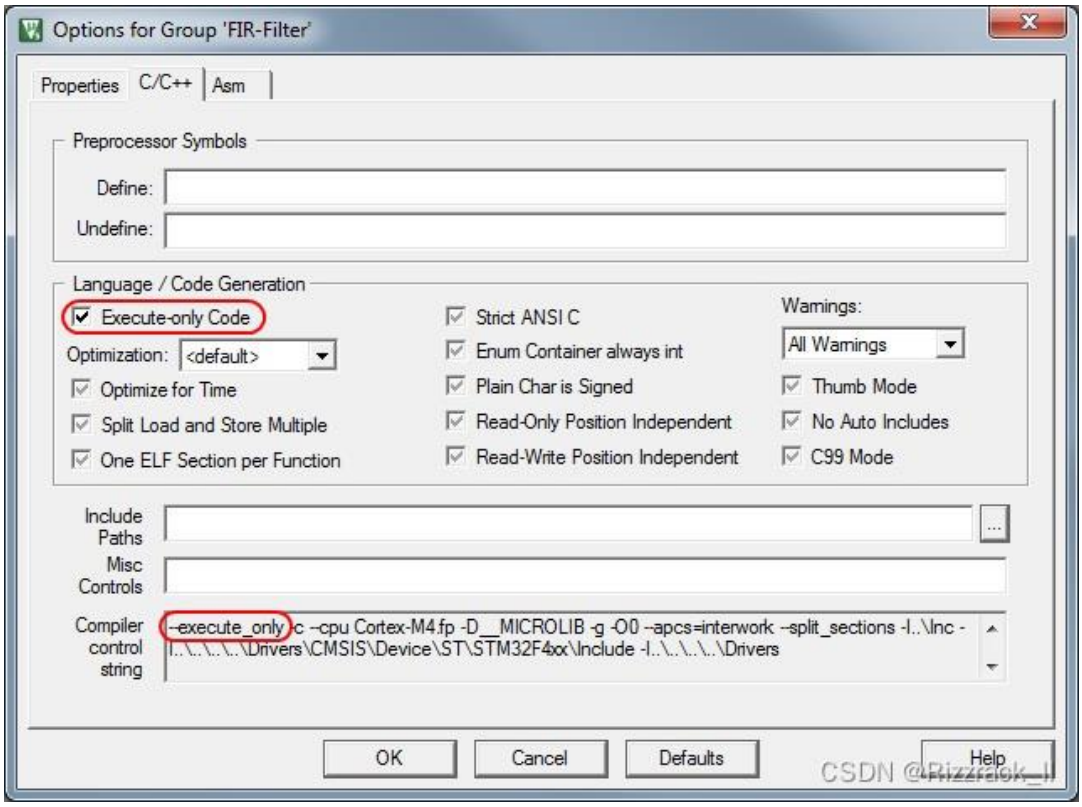
MCU 的中断向量表里都是些常量数据，所以包含中断向量表的扇区不可进行 PCROP。一般来讲向量表放在第一个扇区，所以该扇区不可进行 PCROP。

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)
    }
}
```

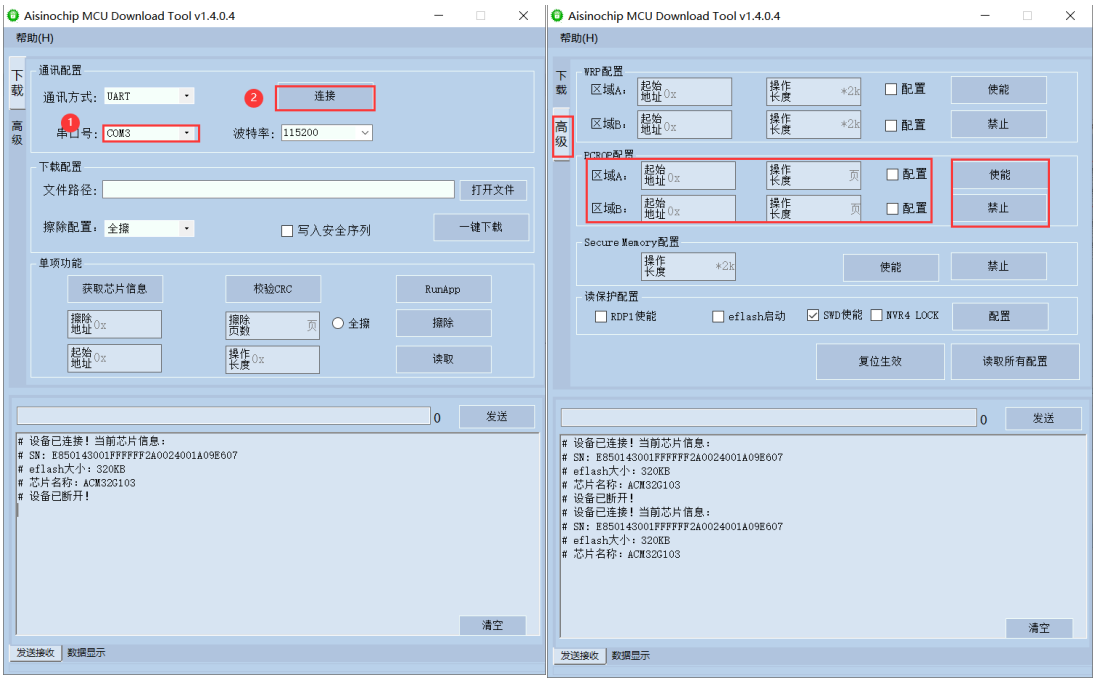
PCROP 保护可以通过下载工具或者在用户代码中使能。

5.1. 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。

RSTN/POR /EFC 复位重启后生效。



5.2. 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 寄存器进行配置。

RSTN/POR /EFC 复位重启后生效。

6. 版本历史

版本	日期	作者	描述
V1.0	2023-05-11	Aisinochip	初始版
V1.1	2024-06-20	Aisinochip	

版权声明

本文档的所有部分，其著作产权归上海航芯电子科技股份有限公司（简称航芯科技）所有，未经航芯科技授权许可，任何个人及组织不得复制、转载、仿制本文档的全部或部分组件。本文档没有任何形式的担保、立场表达或其他暗示，若有任何因本文档或其中提及的产品所有资讯所引起的直接或间接损失，航芯科技及所属员工恕不为其担保任何责任。除此以外，本文档所提到的产品规格及资讯仅供参考，内容亦会随时更新，恕不另行通知。

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