AN4246
应用笔记

STM32L1xx 微控制器上的专有代码读保护

前言

在微控制器领域，对嵌入式代码的知识产权保护已经成为被高度重视的问题。为了提供这方面的保护，STM32 微控制器采用多种不同方法来保护 Flash 代码，避免复制和逆向工程。

本应用笔记描述了通用 STM32 系列的 Flash 保护功能。重点关注 Proprietary Code Read Out Protection（PCROP），它内嵌于中等容量的 STM32L151xC、 STM32L152xC、 STM32L162xC 和 STM32L100xC 微控制器中。

表 1 列出了本应用笔记涉及的微控制器。

表 1. 适用产品

类型	适用产品
微控制器	STM32L1 （STM32L151xC， STM32L152xC， STM32L162xC 和 STM32L100xC）

目录

1 Flash 代码保护

STM32 微控制器系列产品具有下列代码保护功能：

1. 全局读保护 （Read-out Protection， RDP）
2. 写保护
3. 专有代码读保护 （Proprietary Code Read Out Protection， PCROP）

这些功能用来保护嵌入式固件代码的知识产权，这表示对复杂嵌入式系统的关注正在日益增加。

1.1 全局读保护 （RDP）

全局读保护可保护嵌入式固件代码 （预加载到闪存中），避免逆向工程、使用调试工具读出或其他方式的入侵攻击。

该保护在二进制代码载入嵌入式闪存后，由用户进行设置。

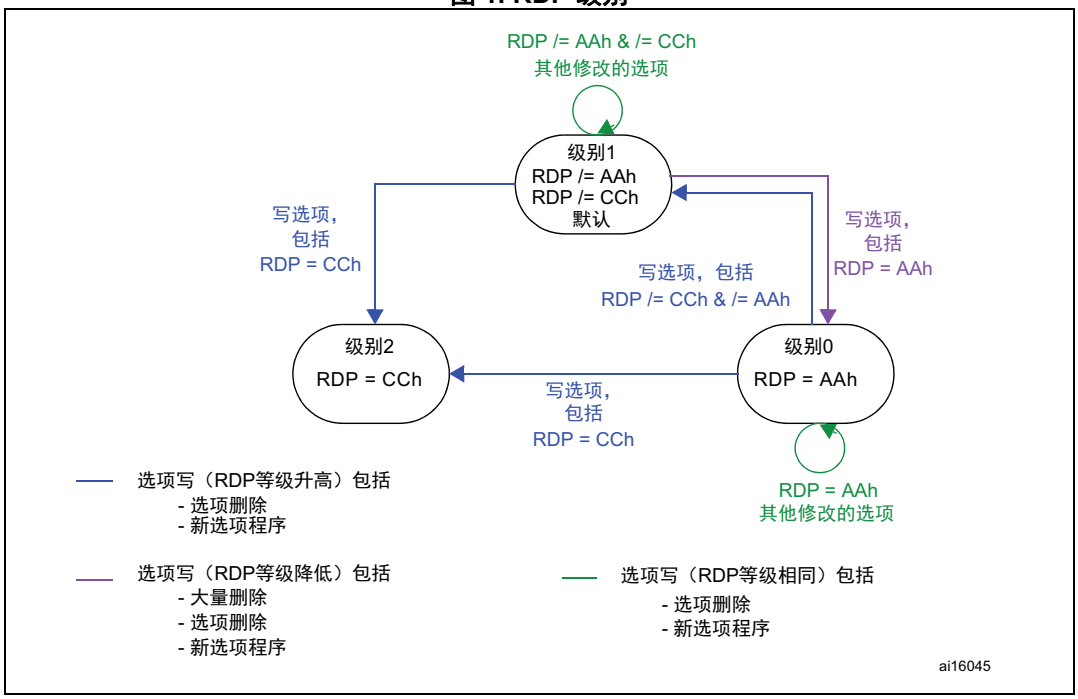
表 2 描述了 3 个用户定义的保护级别。

表 2. RDP 保护级别

级别	说明
级别 0	无保护 （默认）
级别 1	Flash 内存被保护，防止被调试工具读取或者是通过加载到 RAM 中的代码进行读取。
级别 2	所有调试功能被禁用

一旦用户代码被载入闪存中，即可避免代码倾出。可通过激活级别 1 或级别 2 保护来实现，或者通过 RDP 选项字节按照*图 1.* 中所示的准则进行编程。

图 1. RDP 级别



两个保护级别 （1 和 2）都可以保护闪存。其内容不可被 Serial Wire 或 JTAG Debug 访问、自举程序系统软件或通过向易失性 RAM 存储器载入其他软件来读取。

两个保护级别的主要区别在于易失性数据 （RAM 内容）保护，此保护仅存在于级别 2 中。

RDP 保护被设为级别 1 时，调试工具仍然能够连接和访问 MCU （RAM 和寄存器）的所有易失性资源。这些工具通过向 RAM 载入一些测试代码来检查部件和 / 或系统。

并且，级别 1 保护允许通过擦除全部 Flash 内容来恢复已编程部分。可通过将 RDP 选项字节从级别 1 重新编程为级别 0 来实现 （参见*图 1*）。

另一方面，级别 2 保护是不可逆的 （熔断）。一旦 RDP 设为级别 2， RDP 选项字节和所有其他选项字节都会被冻结，不能再修改。

但是，用户 Flash 内容 （除了所有写保护扇区，参见*第 1.2 节：写保护*）在用户代码本身的控制下仍然可被更新。通过执行 IAP （In Application Programming，在应用编程）自举程序代码来允许一些扇区的固件更新。

为了确保能够保护预先编程的用户代码，自举程序协议可以由用户指定 （执行相关保护来避免攻击、倾出和 / 或恶意代码更新）。

注： *利用 STM32 上提供的嵌入式 AES 加速器实现了一些 Secure Bootloader 示例，应用笔记 AN4023 - STM32 安全固件升级中对此有描述。*

关于读保护的更多详细信息，请参考微控制器参考手册。

1.2 写保护

写保护通过 Flash 区 （扇区）实现，可保护指定扇区，避免代码更新或擦除。

利用一个选项位来激活对每个 Flash 扇区的写保护。当设置扇区 *i* （选项位 nWRPi = 0）为写保护时，该扇区不能被擦除或编程。

表 3 显示了对于不同 RDP 级别的扇区写保护。

表 3. 写保护

级别	说明
级别 0 或 1	其他的选项字节仍可被修改。(1)
级别 2	所有的选项字节都被明确冻结。(2)

1. 扇区写保护对于安全功能来说非常重要。如果它们在写保护扇区进行编程，这些功能可受到充分地保护，不会意外擦除或更新。
2. 写保护扇区不可被擦除或修改，无论意外与否。

注： *这种情况下，写入这些扇区的嵌入式固件的完整性可确保不被修改。*

1.3 专有代码读保护

专有代码读保护 （PCROP）是一种替代保护，也是通过扇区实现，可保护特定代码 （知识产权）不受攻击。

PCROP 在微控制器代码保护和代码管理上实现了 2 种主要功能。

表 4 中将两种 PCROP 功能分别与 RDP 保护方法进行了对比。

表 4. 针对攻击的保护

保护类型	对比
外部攻击	与 RDP 提供的保护类似 （但是此保护仅限于特定 Flash 区域）
内部攻击 （如特洛伊木马类型）	应用中可能使用一些 “ 不保险的 ” 的第三方代码，但是仍然保留了部分代码的隐私性

这种保护基于一种只执行机制。 Flash 代码区域仅能被 STM32 CPU （作为指令代码）获取，而所有其他访问 （DMA，调试和 CPU 数据读取）是严格禁止的。

在保护可执行代码不被读取时，这种只执行机制会产生一种副作用，导致被保护代码本身（从该区域执行）不能访问存储在相同区域的相关数据值 （如文字库）。为了避免该区域中数据访问的需要 （特别是文字库访问），必须在 ARM/Keil 编译器中选择一个特殊的命令行选项：
(`armcc --no_literal_pools --max_string_in_code = 0`).

此命令行选项使用其他指令转换文字库操作。这些指令可创建寄存器值，而无需任何数据读取访问。它主要用于载入地址可变寄存器。由于替代方法效率较低，此选项将这些操作转换为效率略低的代码。但性能损失是有限的 （低于 5%），这对于受保护的代码部分来说是可接受的。

利用与写保护同样的选项字节来选择 PCROP 扇区。因此这 2 个选项是互斥的。但是，受保护不被读取的扇区 （PCROP）也不会被写入 / 擦除。因此， PCROP 可认为是扇区写保护的超集。

为了激活 PCROP （改变 nWRP 选项位的功能），必须激活 SPRMOD 选项位。该操作是不可逆的。

同样在 PCROP 模式下，设置为读保护的扇区也不能被复位成无保护状态。因此，新扇区可成为读保护区 （当 RDP 设为级别 0 或 1 时），但是被保护的扇区不能通过擦除或修改成为无保护区。

根据 RDP 级别，存在可能的变通方案来恢复受保护芯片。若 STM32 处于 RDP 级别 1 且 RDP 选项字节设为级别 0，则用户 Flash 区域将被完全擦除。这是 SPRMOD 和 nWRP 位可被复位、所有受保护扇区成为无保护的唯一一种情形。

但是，由于此操作总是与用户 Flash 区域的全局擦除相关联，因此代码保护不受影响。

当 RDP 设为级别 2，所有选项字节都会被冻结，不能再修改。因此，受保护扇区不能再被擦除或修改，这样就成为永久性保护。

2 示例

2.1 安全固件更新 （SFU）自举程序保护

可包含安全固件更新自举程序 （如 AN4023 中所述）。允许在 STM32 闪存中对第三方代码进行编程，而不损害安全自举程序机制和 / 或密钥。

2.2 预加载第三方 IP 代码

可以在 STM32 闪存中预加载 （如通过快速 ROM 程序）包含关键知识产权代码的第三方代码，通过激活 PCROP 机制来保护其不被读取。

这样含有保护代码的 STM32 微控制器可由用户使用 / 编程，而不会影响被保护代码。

3 结论

STM32 微控制器提供了多种 Flash 保护机制来满足知识产权保护的不同需要。这些保护机制从单个用户全局代码保护到细粒度代码保护（多个 IP 固件可共同存在于 STM32 微控制器内存中）。该解决方案允许应用工作于潜在危险的环境中，而不影响代码保护或其完整性。

4 参考文档

编程手册 （PM0062），意法半导体

参考手册 （RM0038），意法半导体

5 版本历史

表 5. 文档版本历史

日期	版本	变更
2013 年 4 月 3 日	1	初始版本。

表 6. 中文文档版本历史

日期	版本	变更
2015 年 12 月 1 日	1	中文初始版本。

重要通知 - 请仔细阅读

意法半导体公司及其子公司 （“ST”）保留随时对 ST 产品和 / 或本文档进行变更、更正、增强、修改和改进的权利，恕不另行通知。买方在订货之前应获取关于 ST 产品的最新信息。 ST 产品的销售依照订单确认时的相关 ST 销售条款。

买方自行负责对 ST 产品的选择和使用， ST 概不承担与应用协助或买方产品设计相关的任何责任。

ST 不对任何知识产权进行任何明示或默示的授权或许可。

转售的 ST 产品如有不同于此处提供的信息的规定，将导致 ST 针对该产品授予的任何保证失效。

ST 和 ST 徽标是 ST 的商标。所有其他产品或服务名称均为其各自所有者的财产。

本文档中的信息取代本文档所有早期版本中提供的信息。