AN1815
应用笔记

UM324xF Flash 读保护使用指南

版本：V1.1

广芯微电子（广州）股份有限公司

http://www.unicmicro.com/

条款协议

1. 本文档中所记载的关于电路、软件和其他相关信息仅用于说明半导体产品的操作和应用实例。用户如在设备设计中应用本文档中的电路、软件和相关信息，请自行负责。对于用户或第三方因使用上述电路、软件或信息而遭受的任何损失，广芯微电子不承担任何责任。
2. 在准备本文档所记载的信息的过程中，广芯微电子已尽量做到合理注意，但是，广芯微电子并不保证这些信息都是准确无误的。用户因本文档中所记载的信息的错误或遗漏而遭受的任何损失，广芯微电子不承担任何责任。
3. 对于因使用本文档中的广芯微电子产品或技术信息而造成的侵权行为或因此而侵犯第三方的专利、版权或其他知识产权的行为，广芯微电子不承担任何责任。本文档所记载的内容不应视为对广芯微电子或其他人所有的专利、版权或其他知识产权作出任何明示、默示或其它方式的许可及授权。
4. 使用本文档中记载的广芯微电子产品时，应在广芯微电子指定的范围内，特别是在最大额定值、电源工作电压范围、热辐射特性、安装条件以及其他产品特性的范围内使用。对于在上述指定范围之外使用广芯微电子产品而产生的故障或损失，广芯微电子不承担任何责任。
5. 虽然广芯微电子一直致力于提高广芯微电子产品的质量和可靠性，但是，半导体产品有其自身的具体特性，如一定的故障发生率以及在某些使用条件下会发生故障等。此外，广芯微电子产品均未进行防辐射设计。所以请采取安全保护措施，以避免当广芯微电子产品在发生故障而造成火灾时导致人身事故、伤害或损害的事故。例如进行软硬件安全设计（包括但不限于冗余设计、防火控制以及故障预防等）、适当的老化处理或其他适当的措施等。

目录

1 摘要

本篇应用笔记主要介绍 UM324xF 对 Flash 中用户代码如何实施读保护，防止用户代码和数据被读取。

本篇应用笔记主要包括：

- 用户选项区域
- Flash读保护
- 低等级读保护开启流程
- 低等级读保护解除流程

注：具体功能及寄存器的操作等相关事项请以用户手册为准。

2 用户选项区域

2.1 选项字节说明

地址 0x04000000 ~ 0x04001FFF 为用户选项页，其中部分地址具有特殊功能，如下表所示：

表 2-1：特殊功能地址说明

名称	地址	位宽	内容
READ_PROTECT	0x04001FC0	8bit	0xAA（默认）：级别 0，无保护 0xCC：级别 2，高等级保护（芯片保护，禁止调试和从 SRAM 启动）（慎重使用！） 其他值：级别 1，低等级保护（存储器读保护，调试功能受限）
BOOT_SOURCE	0x04001FD0	32bit	选择系统上电或复位后从哪个储存器启动： 0x55AA77EF：Flash main 区 其它：Bootloader 启动
OPTION_ZONE_LOCK	0x04001FFC	32bit	选项区域锁定： 55AA77EF：锁定选项区域，无法编程或擦除（慎重使用！） 其它：选项区域可以编程或擦除。

注：选项区域的内容会在 EFC 复位后生效。

2.2 选项字节编程

1. 配置 EFC_CTRL 寄存器，选择单次编程模式，可以选择打开编程校验。
2. 操作 EFC_SEC 寄存器解锁一次写入操作。
3. 对需要编程的地址写入编程数据。

2.3 用户选项区擦写

用户选项区域默认是可以正常操作的，如果用户操作 OPTION_ZONE_LOCK 选项字将选项区域锁定，需用特殊权限解锁选项区域的擦写。

3 Flash 读保护

可对Flash中的用户区域实施读保护，以防不受信任的代码读取其中的数据。读保护分三个级别，具体定义如下：

- **级别 0：无读保护（默认）**

将0xAA写入读保护选项字节（READ_PROTECT）时，读保护级别即设为0。此时，Bootloader和Flash启动时，或者程序运行在SRAM中时，或者通过JTAG/SWD调试接口，均可执行对Flash的读/写操作（如果未设置写保护）。

- **级别 1：低等级保护（存储器读保护，调试功能受限）**

将任意值（0xAA 和 0xCC 以外的值）写入 READ_PROTECT 选项字节时，即激活读保护级别 1。设置读保护级别 1 后：

1. 通过 JTAG/SWD 调试接口或者程序运行在 SRAM 中，或者从 Bootloader 启动时，不能对 Flash、OTP 区进行访问（读取、擦除、编程）。读请求将导致总线错误。
2. 从 Flash 启动时，允许通过用户代码对 Flash、OTP 区进行访问（读取、擦除、编程）。
3. 激活级别 1 后，如果将保护选项字节（READ_PROTECT）改写为级别 0，会自动全部擦除 Flash main 区数据。因此，在取消读保护之前，用户代码区域会清零。当提高保护级别（0->1、1->2、0->2）时，不会执行批量擦除。

- **级别 2：高等级保护（芯片保护，禁止调试和从 SRAM 启动）**

将 0xCC 写入 READ_PROTECT 选项字节时，可激活读保护级别 2。设置读保护级别 2 后：

1. 级别 1 提供的所有保护均有效。
2. 禁止从 Bootloader 和 SRAM 启动。
3. 用户选项字节不能再进行更改。
4. 从 Flash 启动时，允许通过用户代码对 Flash 进行访问（读取、擦除、编程）。

存储器读保护级别 2 是不可更改的。激活级别 2 后，保护级别不能再降回级别 0 或级别 1。

注意：激活级别 2 后，将永久性禁止 JTAG 端口（相当于 JTAG 熔断）。这样，将无法执行边界扫描。广芯微无法对设为保护级别 2 的器件做失效分析。

4 低等级读保护开启流程

1. 使用特殊权限解锁选项区域的擦写。

```
Unlock_Option_ReadWrite();
```

2. 使用回写接口向 READ_PROTECT 地址写入任意值（0xAA 和 0xCC 以外的值）。

(以 0xFF 为例)：

```
eflash_rewrite_word(0x4000000+0x1FC0, 0xFF);  或
HAL_FLASH_RewriteWord(0x4000000+0x1FC0,0xFF);
```

3. 断电后再次上电，低等级读保护生效。

5 低等级读保护解除流程

通过 SWD 下载代码，下载算法里面会清除读保护功能，自动擦除 Flash main 区全部数据。

6 版本维护

版本	日期	描述
V1.0	2023.11.11	初始版
V1.1	2023.12.19	新增低等级读保护具体使用流程