SinoMCU 应用笔记

AN2003

MC51F003A4

分区加密说明

V1.0

上海晟矽微电子股份有限公司

Shanghai SinoMCU Microelectronics Co., Ltd.

目录

1 应用说明

1.1 概述

分块块加密是指，将 ROM 空间等分为四个分区加密块，根据 FLASH ROM 空间地址从低字节到高字节依次递增排列，将每个分区块进行加密。具体分区详见 1.2 相关控制位说明。

注意：此加密并非传统意义上的加密，而是指用户对于 FLASH 区的操作权限，共分为三种操作权限：1、FLASH 分区块不加密，用户可读可写。2、分区块一级加密，FLASH 分区块禁止外部编程器/调试器读出，但允许内部指令在脱机状态下的读出，“调试”情况下无效。3、分区块二级加密，FLASH 分区块禁止内部及外部的的读出。

1.2 相关控制位说明

SCnP(n=0～3)	**FLASH 分区保护控制位：** 1. n 分区加密块不加密：对应的 n 分区加密块无限制，FLASH 内容可正常读出； 2. n 分区加密块一级加密：对应的 n 分区一级加密限制，FLASH 内容禁止外部调试器/编程器读出，但允许内部 MOVC 指令在“脱机”情况下的读出、“调试”情况下无效； 3. n 分区加密块二级加密：对应的 n 分区二级加密限制，FLASH 内容禁止外部调试器/编程器读出，同时禁止内部 MOVC 指令任何情况下的读出； 注意：该芯片中，每 4K 字节大小设定为一个分区加密块，根据 FLASH ROM 空间地址从低字节到高依次递增排列，即 SC0P 对应 0x0000～0x0FFF 区域，SC1P 对应 0x1000～0x1FFF 区域，SC2P 对应 0x2000～0x2FFF 区域，SC3P 对应 0x3000～0x3FFF 区域。

1.3 具体控制介绍

1.3.1 分区块加密区别

一级加密与二级加密的区别：一级加密，只可用内部 MOVC 指令在非调试状态下，读取加密区的内容；二级加密，在任何情况下，都不允许读取加密区的内容。

1.3.2 分区块不加密

Option 配置项中配置不加密如图 1，此时，用户对于整个 FLASH 区间都有读出权限。具体测试现象如下，不加密时，FLASH 区的内容可以读取到 EEPROM 中，如图 2、图 3.

图 1

图 2（FLASH 区）

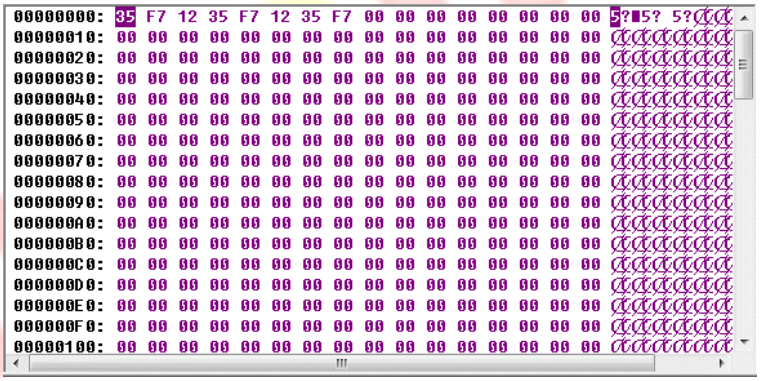

图 3（EEPROM 区）

由图 2、图 3 可知，可将 FLASH 区的内容读取到 EEPROM 中。

1.3.3 分区块一级加密

Option 项中配置用户程序区 0x0000~0xFFFH，一级加密，如图 4，此时，用户对于 0x0000~0x0FFFH 区域（第 0 分区块）中只有在内部指令 MOVC 且在脱机状态下的读取权限，调试状态下无读出权限；其它程序区块可正常读出，不受影响。具体现象如下：FLASH 区（0x0000~0x0FFFH）的内容仅可以通过内部 MOVC 指令在脱机状态下可以读取到 EEPROM 中，如图 5、图 6。且烧录界面中第 0 分区块是被加密为 0 的，但保存不受影响，依然是源文件。

图 4

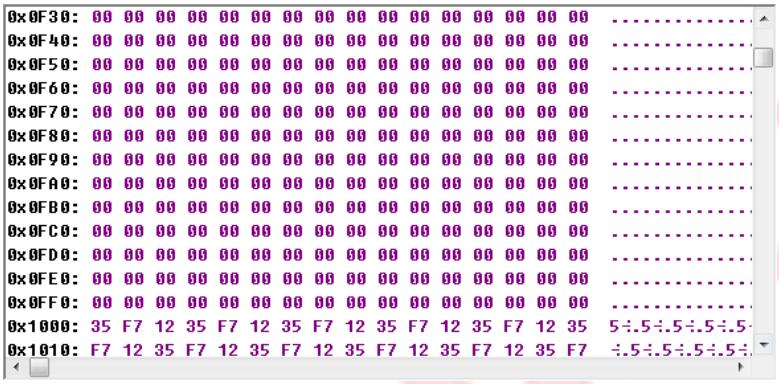

图 5(FLASH 区)

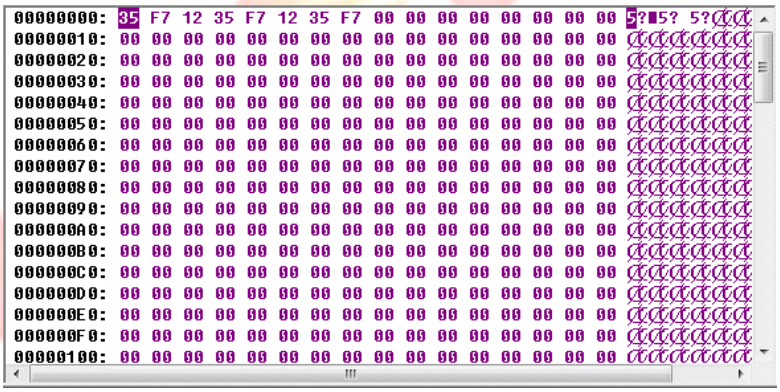

图 6（EEPROM 区）

由图 5、图 6 可知，可将 FLASH 中的内容通过内部 MOVC 指令读取 EEPROM 中去。

1.3.4 分区加密块二级加密

Option 项中配置用户程序区 0x0000~0xFFFH，二级加密，如图 7，此时，用户对于 0x0000~0x0FFFH 区域中的内容无读出权限。但对于其它程序区块有读出权限，不受程序块 0 的影响。具体现象如下，FLASH 区（0x0000~0x0FFFH）的内容使用内部 MOVC 指令也无法读取到 EEPROM 中，FLASH 区的内容是被加密为 0 的，但保存不受影响。如图 8、图 9 所示。

图 7

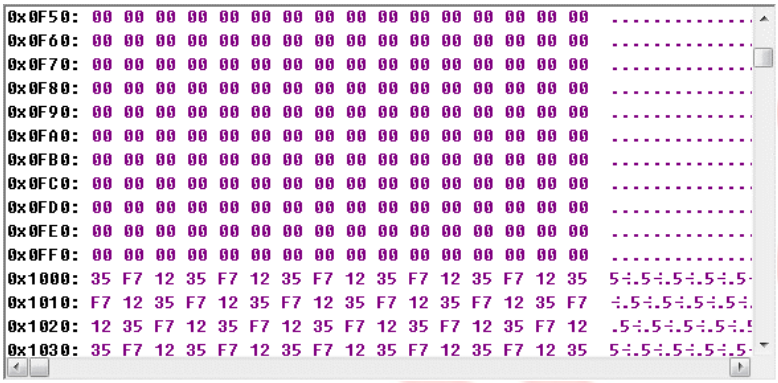

图 8（FLASH 区）

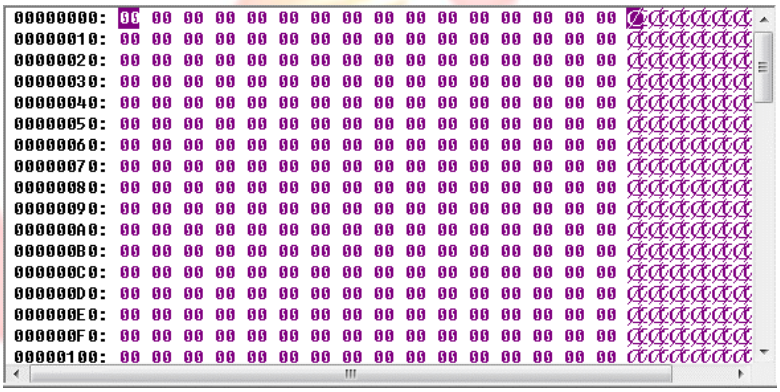

图 9（EEPROM 区）

由图 8、图 9 可知，分区块二级加密时，无法读取 FLASH 区的内容。

2 修订记录

版本	修订日期	修订内容
V0.1	2020-04-13	初版作成；
V0.1	2020-04-14	增加具体说明；