Application Note

SPC11x8_SPD11x8 Security 使用指南

Revision 2 – April 2020

目录

1 引言 5

2 Security 功能 6

2.1 分区保护 6

2.2 Secure Boot 11

2.3 Debug 锁定 11

2.4 随机码保护 11

3 修订历史 12

表格列表

表 2-1： Configuration Words 字段定义 8
表 3-1： 文档修订历史 12

图片列表

图 2-1： Flash 存储器和 IRAM 分区示意图 6
图 2-2： ISP 下载工具 Configuration Words 配置界面 7
图 2-3： ISP 下载工具 Configuration Words 配置项说明 8

1 引言

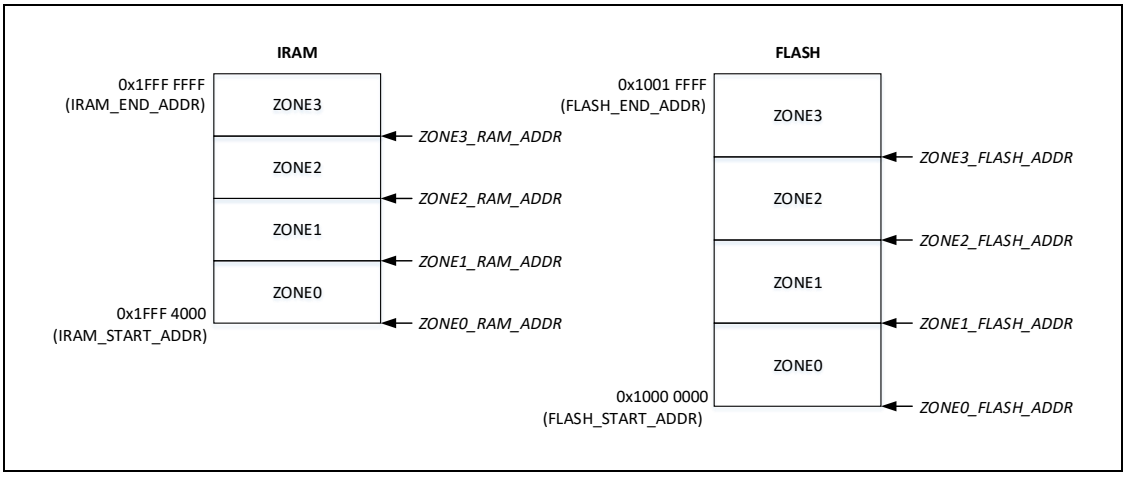
为了降低芯片内部程序被窃取的风险，很多芯片都带有片内程序保护措施。SPC11x8/SPD11x8 在设计之初就考虑到了程序保护的重要性，不仅为用户提供了非常强大而可靠的程序保护措施，还可以让多个合作方安全地共享芯片内部资源。这些措施包括分区保护、Secure Boot、Debug 锁定以及随机码保护。

2 Security 功能

2.1 分区保护

分区保护（Multi-zone Protect）功能能够保证多个合作方在共享芯片的内部资源的同时，不会将程序暴露给任何一个合作方。一旦某个分区的保护被使能，其他分区中的程序就不能够读取或者修改该分区中数据，只能跳转到该分区执行程序。在 SPC11x8/SPD11x8 中，Flash 存储器和 IRAM 最多可以使能 4 个分区的保护功能。用户可以通过设置 Flash 中的 Configuration Words 来使能分区保护。Configuration Words 的具体定义如表 2-1 所示。Flash 存储器和 IRAM 的分区示意图如图 2-1 所示。

图 2-1： Flash 存储器和 IRAM 分区示意图



在图 2-1 中，ZONEx_FLASH_ADDR（x = 0, 1, 2, 3）为 Flash 存储器分区 x（FLASH_ZONEx）的起始地址，需要说明的是，ZONE0_FLASH_ADDR 固定为 Flash 存储器的起始地址，即 0x1000 0000；ZONE0_RAM_ADDR 亦固定为 IRAM 的起始地址。

用户可以通过 Configuration Words 中 ZONEx_FLASH_PROT 字段使能分区 FLASH_ZONEx；通过 ZONEx_RAM_PROT 字段使能分区 RAM_ZONEx。在上文中提到，如果某个分区使能后，其他分区中的程序就不能够读取或者修改该分区中的数据。但是有一个例外情形，如果分区 FLASH_ZONEx 和 RAM_ZONEx（x 为同一个值）都被使能，那么这两个分区中的程序是可以相互访问（读/写）对方的。例如，FLASH_ZONE0 和 RAM_ZONE0 都被使能，那么 FLASH_ZONE0 可以访问 RAM_ZONE0 中的内容，同时 RAM_ZONE0 也可以访问 FLASH_ZONE0 中的内容。

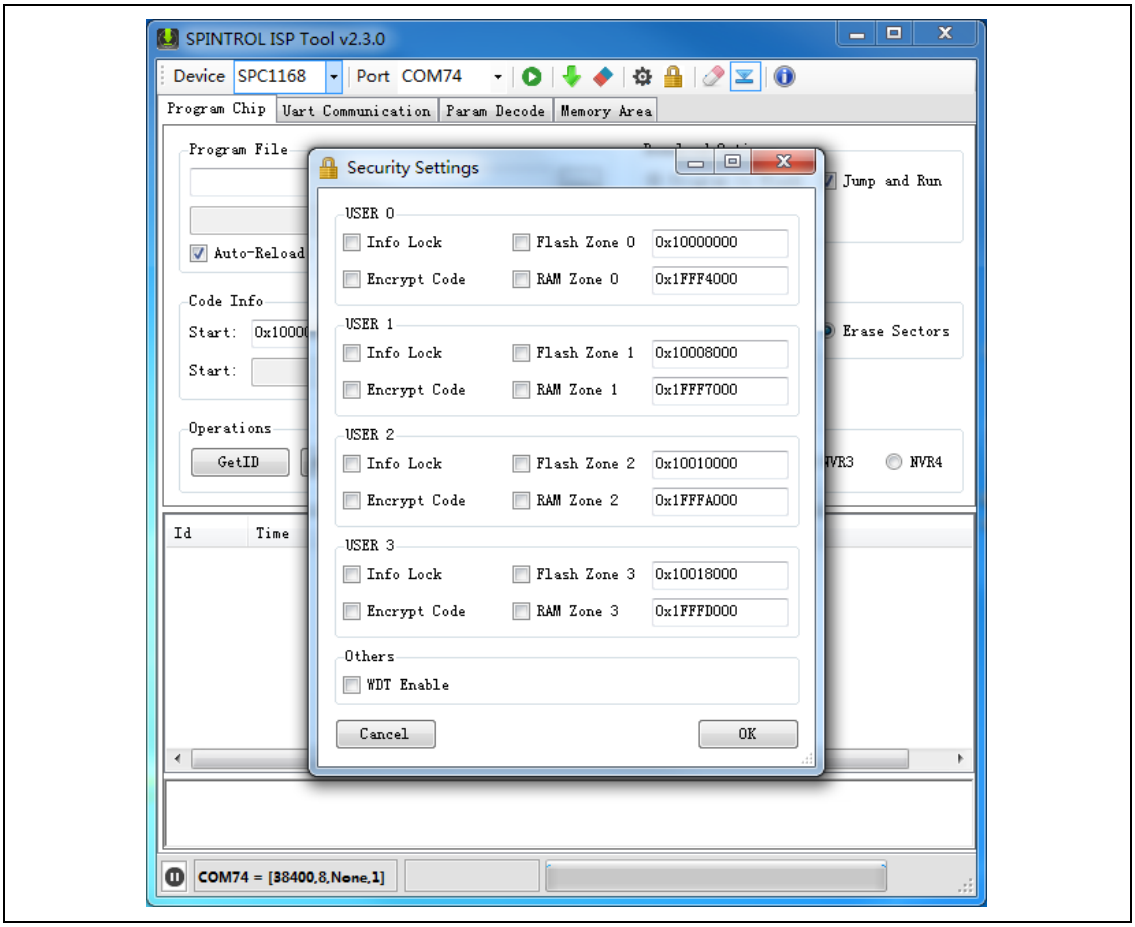
Flash 存储器分区 FLASH_ZONEx 的大小由下列因素决定（y = x + 1）：

- FLASH_ZONEx 和 FLASH_ZONEy 都使能了分区保护，则 FLASH_ZONEx 的大小为（ZONEy_FLASH_ADDR - ZONEx_FLASH_ADDR）。例如，FLASH_ZONE0 和 FLASH_ZONE1 都使能了分区保护，则 FLASH_ZONE0 大小为（ZONE1_FLASH_ADDR – ZONE0_FLASH_ADDR）；
- FLASH_ZONEx 使能了分区保护，FLASH_ZONEy 未使能分区保护，则 FLASH_ZONEx 的大小由 FLASH_ZONEz（z > y）的保护状态决定（FLASH_ZONEz 为满足条件 z > y 的任意一个分区）：

  - FLASH_ZONEz 使能了分区保护，则 FLASH_ZONEx 的大小为（ZONEz_FLASH_ADDR - ZONEx_FLASH_ADDR）。此时，ZONEy_FLASH_ADDR = ZONEz_FLASH_ADDR，FLASH_ZONEy 的大小为 0；
  - FLASH_ZONEz 未使能分区保护，则 FLASH_ZONEx 的大小为（FLASH_END_ADDR + 1 - ZONEx_FLASH_ADDR ）。此时 ZONEy_FLASH_ADDR = ZONEz_FLASH_ADDR = FLASH_END_ADDR，FLASH_ZONEy 和 FLASH_ZONEz 的大小均为 0；
- FLASH_ZONEx 未使能分区保护，FLASH_ZONEy 使能了分区保护，则 FLASH_ZONEx 的大小由 FLASH_ZONEx 是否为 FLASH_ZONE0 决定：
  - FLASH_ZONEx 是 FLASH_ZONE0，则 FLASH_ZONEx 的大小为（ZONEy_FLASH_ADDR – ZONE0_FLASH_ADDR）；
  - FLASH_ZONEx 不是 FLASH_ZONE0，则 FLASH_ZONEx 的大小为 0。

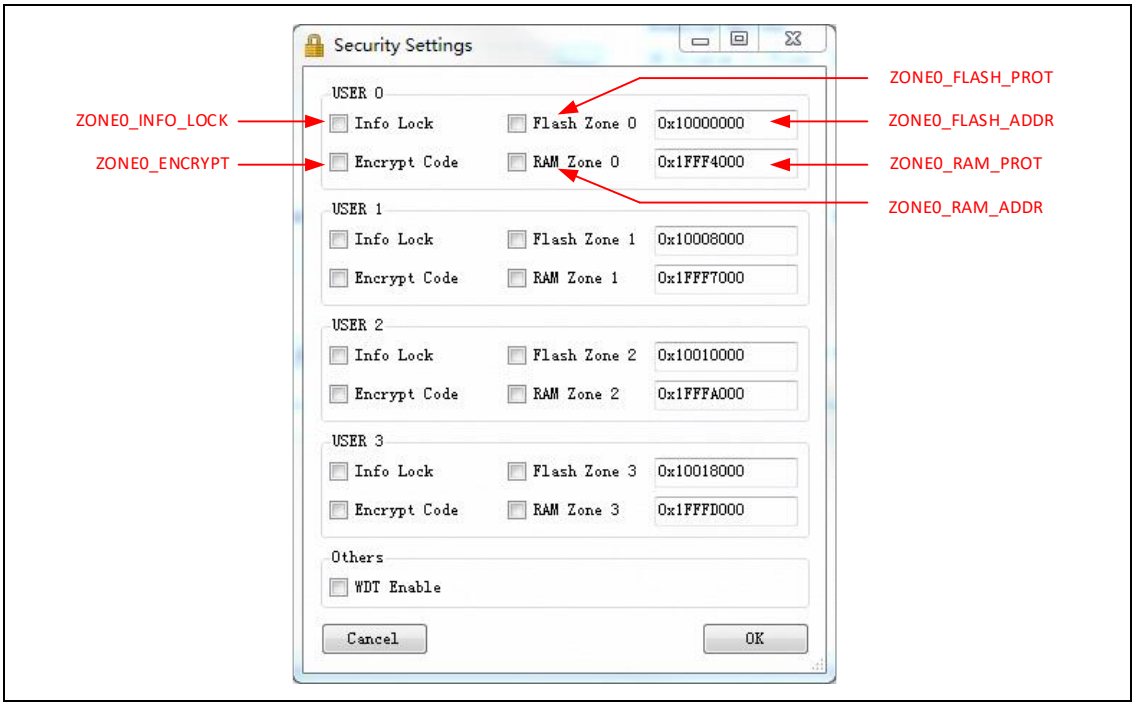
决定存储器分区 FLASH_ZONEx 的大小的规则，同样适用于 IRAM 的分区 RAM_ZONEx 大小的确定。SPINTROL 提供的 ISP 下载工具可以帮助用户设置 Configuration Words，界面如图 2-2 所示。

图 2-2： ISP 下载工具 Configuration Words 配置界面



在图 2-3 中，USER x 用于设置分区 x（x = 0, 1, 2, 3）的 Security 功能，图中也标识出了 USER x 各个配置项和表 2-1 所示字段的对应关系（以 USER 0 为例）。

图 2-3： ISP 下载工具 Configuration Words 配置项说明



Configuration Words 存放在芯片内部的 Flash 模块中，每个分区相关的字段定义和地址如下表所示。

表 2-1： Configuration Words 字段定义

地址	名称	功能及说明
0x11000600	ZONE0_INFO_LOCK	Lock the Configuration Words of zone 0 (0x11000600 – 0x1100063F) 0xFFFFFFFF: The Configuration Words of zone 0 can't be programmed Others: The Configuration Words of zone 0 can be programmed
0x11000604	ZONE0_ENCRYPT	Encrypt status of code in Flash zone 0 0xDEC0DE: The code in Flash zone 0 has been encrypted Others: The code in Flash zone 0 is raw code
0x11000608	ZONE0_DECRYPT	Decrypt status of code in Flash zone 0 0xAA621623: Success to decrypt code in Flash zone 0 0x1E55051: Fail to decrypt code in Flash zone 0 Others: Not valid
0x1100060C	ZONE0_FLASH_PROT	Flash zone 0 protection word 0xFFFFFFFF: Disable Flash zone 0 protection Others: Enable Flash zone 0 protection
0x11000610	ZONE0_FLASH_ADDR	Flash zone 0 start address

地址	名称	功能及说明
0x11000614	ZONE0_RAM_PROT	RAM zone 0 protection word 0xFFFFFFFF: Disable RAM zone 0 protection Others: Enable RAM zone 0 protection
0x11000618	ZONE0_RAM_ADDR	RAM zone 0 start address
0x1100061C ~ 0x1100063F	Reserved for ZONE0	Reserved Configuration Words for ZONE 0
0x11000640	ZONE1_INFO_LOCK	Lock the Configuration Words of zone 1 (0x11000640 – 0x1100067F) 0xFFFFFFFF: The Configuration Words of zone 1 can't be programmed Others: The Configuration Words of zone 1 can be programmed
0x11000644	ZONE1_ENCRYPT	Encrypt status of code in Flash zone 1 0xDEC0DE: The code in Flash zone 1 has been encrypted Others: The code in Flash zone 1 is raw code
0x11000648	ZONE1_DECRYPT	Decrypt status of code in Flash zone 1 0xAA621623: Success to decrypt code in Flash zone 1 0x1E55051: Fail to decrypt code in Flash zone 1 Others: Not valid
0x1100064C	ZONE1_FLASH_PROT	Flash zone 1 protection word 0xFFFFFFFF: Disable Flash zone 1 protection Others: Enable Flash zone 1 protection
0x11000650	ZONE1_FLASH_ADDR	Flash zone 1 start address
0x11000654	ZONE1_RAM_PROT	RAM zone 1 protection word 0xFFFFFFFF: Disable RAM zone 1 protection Others: Enable RAM zone 1 protection
0x11000658	ZONE1_RAM_ADDR	RAM zone 1 start address
0x1100065C ~ 0x1100067F	Reserved for ZONE1	Reserved Configuration Words for ZONE 1
0x11000680	ZONE2_INFO_LOCK	Lock the Configuration Words of zone 2 (0x11000680 – 0x110006BF) 0xFFFFFFFF: The Configuration Words of zone 2 can't be programmed Others: The Configuration Words of zone 2 can be programmed
0x11000684	ZONE2_ENCRYPT	Encrypt status of code in Flash zone 2 0xDEC0DE: The code in Flash zone 2 has been encrypted Others: The code in Flash zone 2 is raw code
0x1100688	ZONE2_DECRYPT	Decrypt status of code in Flash zone 2 0xAA621623: Success to decrypt code in Flash zone 2 0x1E55051: Fail to decrypt code in Flash zone 2 Others: Not valid
0x1100068C	ZONE2_FLASH_PROT	Flash zone 2 protection word

地址	名称	功能及说明
		0xFFFFFFFF: Disable Flash zone 2 protection Others: Enable Flash zone 2 protection
0x11000690	ZONE2_FLASH_ADDR	Flash zone 2 start address
0x11000694	ZONE2_RAM_PROT	RAM zone 2 protection word 0xFFFFFFFF: Disable RAM zone 2 protection Others: Enable RAM zone 2 protection
0x11000698	ZONE2_RAM_ADDR	RAM zone 2 start address
0x1100069C ~ 0x110006BF	Reserved for ZONE2	Reserved Configuration Words for ZONE 2
0x110006C0	ZONE3_INFO_LOCK	Lock the Configuration Words of zone 3 (0x110006C0 – 0x110006FF) 0xFFFFFFFF: The Configuration Words of zone 3 can't be programmed Others: The Configuration Words of zone 3 can be programmed
0x110006C4	ZONE3_ENCRYPT	Encrypt status of code in Flash zone 3 0xDEC0DE: The code in Flash zone 3 has been encrypted Others: The code in Flash zone 3 is raw code
0x110006C8	ZONE3_DECRYPT	Decrypt status of code in Flash zone 3 0xAA621623: Success to decrypt code in Flash zone 3 0x1E55051: Fail to decrypt code in Flash zone 3 Others: Not valid
0x110006CC	ZONE3_FLASH_PROT	Flash zone 3 protection word 0xFFFFFFFF: Disable Flash zone 3 protection Others: Enable Flash zone 3 protection
0x110006D0	ZONE3_FLASH_ADDR	Flash zone 3 start address
0x110006D4	ZONE3_RAM_PROT	RAM zone 3 protection word 0xFFFFFFFF: Disable RAM zone 3 protection Others: Enable RAM zone 3 protection
0x110006D8	ZONE3_RAM_ADDR	RAM zone 3 start address
0x110006DC ~ 0x110006FF	Reserved for ZONE3	Reserved Configuration Words for ZONE 3

2.2 Secure Boot

Secure Boot 允许用户的程序以密文的形式写入到芯片内部的 Flash 存储器中。然后，在芯片上电后，bootloader 负责将用户的程序在 Flash 中进行自解密。这样可以避免用户原始程序文件（HEX 文件）在分发过程中泄露程序的风险。SPC11x8/SPD11x8 的 Secure Boot 支持 Flash 存储器每个分区的自解密。

在实际使用中，用户在将加密后的程序烧录到芯片 Flash 存储器中后，需要设置 Configuration Words 中 ZONEx_ENCRYPT 字段的值为 0xDEC0DE，表示该分区中的程序被用户加密了。这样，在芯片重新启动后，bootloader 会将用户的程序进行自解密，如果解密成功，则设置 ZONEx_DECRYPT 的值为 0xAA621623；如果解密失败，则设置 ZONEx_DECRYPT 的值为 0x1E55051。

2.3 Debug 锁定

芯片的 Debug 接口在程序调试和烧录时，需要经常使用到。这也意味着可以通过 Debug 接口读取或者改写芯片内部存储器的内容。因此，在产品量产时，Debug 功能必须被禁用，这样就可以避免通过 Debug 接口去获取芯片内部的程序。当 SPC11x8/SPD11x8 内部的 Flash 存储器或者 IRAM 的任意一个分区保护被使能后，芯片的 Debug 接口就会被锁定。

2.4 随机码保护

有些芯片破解人员也许会具备使用特定设备将芯片打开的能力，然后将 Flash 中的数据读取出来，然后再将这些数据写到未编程的 SPC11x8/SPD11x8 芯片中，实现对用户产品的复制。对于这种情形，SPC11x8/SPD11x8 也具备相应的保护机制。

SPC11x8/SPD11x8 在出厂时会被写入一个 8 字节的随机码，这个随机码一旦写入后，是不可以再被修改的。客户的应用程序在运行时可以从芯片中读取并校验该随机数。如果该随机数与应用程序预设的值不一致，就终止应用程序的运行。由于每个芯片的随机码不相同，即使芯片破解人员获得了 Flash 中的程序数据，然后将这些程序数据写到其他 SPC11x8/SPD11x8 芯片中，程序也不会正常工作。这样，客户的产品就不能够被批量复制。

3 修订历史

表 3-1： 文档修订历史

日期	版本	修改内容
2019-07-24	1	初始版本
2020-04-10	2	1. 增加图 2-3： ISP 下载工具 Configuration Words 配置项说明。