文档编号：AN4507
第 1 版，2012 年 6 月

使用 Kinetis 的安全和闪存保护功能

作者：Melissa Hunter
汽车和工业解决方案事业部

目录

1 介绍

Kinetis 系列微控制器包含系统安全和闪存保护功能，可用于保护代码和数据免遭未经授权的访问或修改。本应用笔记将介绍 Kinetis 系列处理器上配备的安全和闪存保护功能的用法。本应用笔记还涵盖了如何用闪存配置区段控制芯片的安全和闪存保护功能。

默认安全选项是基于应用程序映像在复位时进行配置的。所有的闪存应用程序映像都需要包含这些安全和保护选项的配置。在所有情况下都需要配置。即使所需的设置是去禁用闪存和安全选项，应用程序映像也必须为这些期望值配置相应的设置。因此，任何编写应用程序的人都必须了解安全和保护选项以及如何正确地配置它们。

2 安全与保护

Kinetis 安全功能是系统级选项，旨在防止未经授权的对处理器以及处理器中代码和数据的访问。软件知识产权（IP）是非常宝贵的投资，而安全功能可以保护该投资，防止克隆，并保障可能存储在存储器中的敏感数据的安全。

- 安全功能：虽然 Kinetis 上的安全功能是由驻留在闪存中的设置来控制的，但它并不是闪存级的功能。闪存为芯片系统逻辑提供安全选项，而芯片系统逻辑根据该设置采取行动。因此，即使用户通过与闪存交互来进行安全设置，也必须将其视为一种处理器模式来选择，因为用户所做的决定将影响到整个处理器。事实上，启用或禁用安全功能选项对闪存本身的影响很小。即使启用了安全功能，闪存仍可完全运行。这意味着驻留在闪存中的启用了安全功能的固件仍然可以对闪存进行修改，因为对闪存本身的读取、擦除和编程操作并没有被改变（大规模擦除可能除外）。
- 闪存保护功能：相比之下，闪存保护功能只影响闪存本身。闪存保护旨在防止对闪存区域的意外擦除或编程。该选项只影响对所选闪存区域的修改能力，对处理器的其他部分没有影响。

2.1 安全选项

以下各节将介绍 Kinetis 中配备的安全选项。首先，请查看 http://www.nxp.com.cn 上的 Kinetis 参考手册中的实际寄存器和区段说明，然后详细了解每个选项的工作原理以及如何对它们进行配置。

2.1.1 FSEC 寄存器和区段设置

闪存安全（FSEC）寄存器包含多个区段，用于启用/禁用安全功能，以及用于选择一些在启用安全功能后会生效的功能。图 1 所示为 FSEC 寄存器区段，表 1 所示为每个区段的位设置。以下各节将详细地介绍 FSEC 寄存器中所有的可用选项，包括对系统的影响和推荐的使用方法。

Bit	7	6	5	4	3	2	1	0
Read	KEYEN		MEEN		FSLACC		SEC	
Write								

图 1. 闪存安全寄存器

表 1. FSEC 的区段说明

区段	说明
7–6 KEYEN	启用后门密钥安全功能。 此区段可启用或禁用后门密钥对闪存模块的访问。 00 禁用后门密钥的访问。 01 禁用后门密钥的访问（首选的 KEYEN 状态以禁用后门密钥的访问） 10 启用后门密钥的访问。 11 禁用后门密钥的访问。

表格续下页...

表 1. FSEC 的区段说明（续）

区段	说明
5–4 MEEN	启用大规模擦除 该区段可启用和禁用闪存模块的 JTAG 和 EzPort 的大规模擦除功能。只有在 SEC 区段设置为“安全”时，MEEN 区段的状态才有效。当 SEC 区段设置为“非安全”时，MEEN 设置无效。 00 启用大规模擦除。 01 启用大规模擦除。 10 禁用大规模擦除。 11 启用大规模擦除。
3–2 FSLACC	恩智浦故障分析代码。 在恩智浦对返厂的部件进行故障分析期间，该区段可启用或禁用对闪存内容的访问。当 SEC 为“安全”状态且 FSLACC 为“拒绝”状态时，恩智浦将无法访问闪存内容，而恩智浦工厂的测试要实施的任何故障分析，都必须先进行完全擦除以解除部件的安全状态（假设启用了大规模擦除功能）。 当允许访问时（即 SEC 为“非安全”状态，或 SEC 为“安全”状态且 FSLACC 为“允许”状态），恩智浦工厂测试可查看当前闪存内容。只有当 SEC 设置为“安全”状态时，FSLACC 的状态才有效。当 SEC 设置为“非安全”状态时，FSLACC 的设置无效。 00 允许恩智浦工厂的访问。 01 拒绝恩智浦工厂的访问。 10 拒绝恩智浦工厂的访问。 11 允许恩智浦工厂的访问。
1–0 SEC	闪存安全 该区段定义了 MCU 的安全状态。在安全状态下，MCU 会限制对闪存模块资源的访问。如果使用后门密钥访问，闪存模块转换为非安全状态，则 SEC 区段将强制转换为 10b。 00 MCU 的安全状态为“安全”。 01 MCU 的安全状态为“安全”。 10 MCU 的安全状态为“非安全”，即 MCU 的标准出厂状态为“非安全”。 11 MCU 的安全状态为“安全”。

2.1.1.1 启用/禁用安全功能

在设置 FSEC[SEC] 时，用户必须首先决定是否启用安全功能。以下各节将讨论启用或禁用安全功能所带来的影响。

2.1.1.1.1 启用安全功能对 JTAG 的影响

为了保护处理器内部的信息，当安全功能开启时，访问处理器内部的调试将被禁用。但即使启用了安全功能，也还可以进行 JTAG 的扫描链操作。

可以访问驻留在 JTAG 和调试逻辑中的寄存器，但不能通过调试端口访问处理器内部的其他寄存器或存储器。

即使启用了安全功能，也可以读取 MDM-AP 状态寄存器（它是调试寄存器之一）。该寄存器驻留在调试逻辑内，可用于验证当前的安全设置。这对于解决在与处理器建立调试连接时遇到的问题有一定作用。如果遇到此种问题，则可以使用 MDM-AP 的值来确定是否启用了安全功能并阻止了调试连接。

如果仍然通过 FESC[MEEN] 启用了大规模擦除，则 JTAG 端口也可用于请求大规模擦除。大规模擦除完成后，安全功能将被关闭。这意味着可以使用大规模擦除来恢复调试器与部件的连接，但是在此过程中，闪存中的所有代码/数据都将丢失。

2.1.1.1.2 启用安全功能对 EzPort 的影响

当启用安全功能后，只要 EzPort 模式入口被启用，处理器就仍可启动进入 EzPort 模式。EzPort 通信仍将处于活动状态，可用于发送命令，但许多命令将不被接受。最重要的是，在启用安全功能的情况下，唯一可以读取的资源就是 EzPort 状态寄存器。与 MDM-AP 状态寄存器类似，可以通过读取 EzPort 状态寄存器来确定是否启用了闪存安全功能。

如果 MEEN 区段允许，EzPort 还可以用于执行闪存的大规模擦除，以解除处理器的安全状态。

2.1.1.1.3 启用安全功能对 FlexBus 的影响

当启用安全功能后，FlexBus 操作是可编程的。SIM_SOPT2[FBSL] 用于控制对外部总线的哪些访问是允许的（在启用安全功能后）。默认情况下，启用安全功能后，对 FlexBus 的所有外部访问都会被阻止。有些选项是只允许数据访问，或者同时允许数据和操作码访问。如果同时允许数据和操作码访问，则在启用或禁用安全功能时，FlexBus 控制器的行为方式是相同的。

注意

SIM_SOPT2[FBSL] 仅在启用安全功能时有效。如果禁用了安全功能，则 SIM_SOPT2[FBSL] 无效。

2.1.1.1.4 启用安全功能对闪存的影响

虽然处理器的安全状态是通过闪存块传递到片上系统（SoC）其他部分的，但闪存操作基本上不受安全状态的影响。已存储在存储器内的驻留固件可以在任意一种安全状态下运行相同的闪存命令集。通过固件，用户可以以相同的方式对闪存进行读取、擦除和编程（即使该器件处于安全状态）。由于 EzPort 和 JTAG 的访问受到限制，外部不能对闪存进行访问，但在部件内部，闪存可以正常使用。当使用通信端口进行现场固件升级时，可以启用安全功能，而固件升级代码仍可正常执行。

2.1.1.1.5 禁用安全功能后会发生的情况

如果安全功能被禁用，则此寄存器中的所有其他选项都将被忽略。默认情况下，处理器实际上处于安全状态，但在处理器从闪存中获取安全选项后的复位过程中，如果这样选择了，它将禁用安全功能，并开放调试、EzPort 和 FlexBus 的访问权限。

2.1.1.2 启用后门密钥

FSEC 寄存器中的第二个选项是一个后门密钥的启用选项，它由 FSEC[KEYEN] 控制。当启用后门密钥选项后，如果在执行闪存验证后门访问密钥命令时提供了正确的 64 位密钥值，则后门密钥选项允许暂时禁用闪存安全功能。

2.1.1.2.1 使用后门密钥功能时需注意的重要事项

在使用安全功能时，后门密钥解锁功能是非常实用的；但是，使用该功能需要进行一些预配置。以下是使用后门密钥时需注意的一些重要提示：

- 要在启用安全功能和后门密钥功能的同时，为应用程序配置 64 位对比密钥值。如果不使用固件对闪存的一些部分重新编程并复位器件，则无法在一个已运行的处于安全状态的器件上配置密钥值。
- 全 0 或全 1 不能作为密钥值。所选的密钥值必须是至少包含一个 1 和一个 0 的某种组合。如果用户尝试使用一个全 0 或全 1 的密钥值，则“验证后门访问密钥”命令将会返回错误信息。
- 处理器中没有用于获取密钥值和运行“验证后门访问密钥”命令的预配置机制。应用程序需要包含一个代码序列，以允许用户输入密钥值，然后使用输入的值来运行“验证后门密钥”命令。
- 如果“验证后门访问密钥”命令检测到预编程的对比密钥与提供的密钥之间不匹配，则需要上电复位才能再次执行“验证后门访问密钥”命令。
- 如果“验证后门访问密钥”命令检测到对比密钥与提供的密钥匹配正确，则闪存安全功能将被暂时关闭。一旦处理器复位，除非已经执行操作更改了默认安全设置，否则它将返回到安全状态。

2.1.1.2.2 使用后门密钥解锁安全功能

以下步骤描述了使用后门密钥暂时关闭安全功能的典型操作顺序：

1. 用一个启用了安全功能和后门密钥访问功能的应用程序对处理器上的闪存进行编程，并设置一个有效的后门访问比较密钥值。有关如何配置这些选项的信息，参见如何配置安全选项。应用程序还必须包含在此过程中所描述的执行其他步骤的代码。
2. 最终用户必须执行某些操作，以表明他们想要输入密钥值来暂时关闭安全功能。这可以通过某种形式的串行命令或硬件交互来实现。例如，用户可以使用通过串行终端命令行界面输入的“后门”命令来设置应用程序，或者甚至可以在电路板上设置一个按钮来产生中断，从而使软件分支到一个特殊的后门密钥序列。
3. 当固件检测到用户要暂时解除设备安全状态后，必须提示用户输入 64 位密钥值。通常，这需要使用处理器上的某个通信端口（如 UART、SPI 或以太网）来完成。
4. 等待用户输入 64 位密钥。
5. 当获取了 64 位用户密钥后，将“验证后门访问密钥”命令的命令值和操作数载入到闪存 FCCOBn 寄存器中，如下表所示：

表 2. 验证后门访问密钥命令

FCCOB 号	FCCOB 内容
0	0x45 (VFYKEY)
1–3	未使用
4	用户密钥字节 0
5	用户密钥字节 1

表格续下页...

表 2. 验证后门访问密钥命令（续）

FCCOB 号	FCCOB 内容
6	用户密钥字节 2
7	用户密钥字节 3
8	用户密钥字节 4
9	用户密钥字节 5
A	用户密钥字节 6
B	用户密钥字节 7

注意

请注意字节顺序和 FCCOB 寄存器的位置。该闪存最初是为大端架构设计的，但 Kinetis 是小端架构。为了防止字节交换问题，最好将预配置密钥和用户密钥作为两个 32 位的值来处理，并始终将它们以 32 位格式读写。FCCOB 寄存器是 8 位的寄存器；但使用 32 位格式访问一次可以写入四个寄存器 。

6. 清除闪存中的 FCSR[CCIF] 区段，以开始执行“验证后门访问密钥”命令。
7. 如果用户密钥与对比后门密钥匹配成功，则安全功能将被暂时关闭。

由于这些步骤的大部分由应用程序处理，所以还可以有其他选择。例如，在调试过程中，可以在电路板上设置一个按钮作为解锁按钮。软件能够检测到按钮按下，然后执行“验证后门访问密钥”命令，而不需要用户通过某种方式输入密钥。但是这种方法不太安全，因此不推荐使用。不过，如何正确处理后门密钥，或者是否使用后门密钥，这都完全由用户决定。

2.1.1.3 禁用大规模擦除

第三个安全设置（FSEC[MEEN]）提供了完全禁用闪存大规模擦除功能的选项。禁用大规模擦除功能可以为系统提供更高级别的安全功能。这将防止有人使用 JTAG 或 EzPort 大规模擦除命令来覆盖安全功能并载入一个新的应用程序。但是，这意味着将失去大规模擦除能力。

注意

如果用户在没有使用其他方法解除设备安全状态（没有使用后门密钥，也没有使用改变默认安全选项的固件方法）的情况下禁用了大规模擦除，那么该器件将永远处于安全状态。

注意

即使禁用了大规模擦除，也可以使用闪存的“擦除所有块”命令来大规模擦除该器件。这是一个闪存命令，需要器件中的固件才能执行该命令。

2.1.1.4 禁用恩智浦访问

FSEC[FSLACC]决定了当器件处于安全状态时，恩智浦是否能访问该器件。如果存在可疑的质量问题，并且部件被退回到恩智浦进行重新测试和故障分析，则需要重点关注此区段。下表列出了恩智浦访问的条件。

表 3. 恩智浦访问的条件

如果	那么
器件处于安全状态，同时禁用了恩智浦访问且启用了大规模擦除功能	恩智浦将通过大规模擦除器件以解除其安全状态，从而开始故障分析流程。
器件处于安全状态，同时禁用了恩智浦访问并关闭了大规模擦除功能	恩智浦对器件进行故障分析的能力非常有限。因此，如果用户计划禁用恩智浦访问，建议保留启用大规模擦除功能。

2.1.2 如何配置安全选项

正如介绍中提到的，应用程序映像本身决定了默认的安全选项。这是通过对闪存阵列中的特定位置（即闪存配置区段）进行编程来完成的。在复位过程中，闪存逻辑会读取那些被编程到该闪存配置区段位置（0x400-0x40F）的值，并使用这些值来获取多个闪存寄存器的默认值，同时将一些设置信息传递给 SoC。

注意

由于应用程序映像负责设置默认安全选项，因此所有的闪存映像都必须包含有效的闪存配置数据。如果在对闪存编程时未能正确配置闪存配置区段，那么可能会导致处理器永久处于安全状态。

表 4 所示为所有闪存配置区段的地址，并简要说明了每个位置的使用方法。有关闪存配置区段和闪存寄存器（包括位定义）的完整说明，请参见 http://www.nxp.com.cn 上提供的特定 Kinetis 器件的参考手册。

表 4. 闪存配置区段

闪存配置区段地址	大小（字节）	区段说明	按区段初始化的闪存寄存器
0x400–0x407	8	后门对比密钥。 详见启用后门密钥	
0x408–0x40B	4	默认程序闪存保护设置	FPROT0–3
0x40F	1	默认数据闪存保护设置。此设置仅用于 FlexNVM 器件。对于仅使用 P-Flash 的器件，该区段未使用（写为 0xFF）。	FDPROT
0x40E	1	默认 EEPROM 保护设置。此设置仅用于 FlexNVM 器件。对于仅使用 P-Flash 的器件，该区段未使用（写为 0xFF）。	FEPROT

表格续下页...

表 4. 闪存配置区段（续）

闪存配置区段地址	大小（字节）	区段说明	按区段初始化的闪存寄存器
0x40D	1	闪存选项字节。该区段用于配置 SoC 特定设置。这些选项在不同的 Kinetis 器件上会有所不同。请参见 http://www.nxp.com.cn 上特定 Kinetis 器件的参考手册，以查看可用于该处理器的设置。	FOPT
0x40C	1	默认的闪存安全寄存器设置。	FSEC

注意

下载到处理器的所有闪存映像都必须包含闪存配置区段的对应值，这一点极为重要。恩智浦建议在矢量表的最后添加闪存配置区段值。矢量表存储在 0x0-0x3FF，然后闪存配置区段为 0x400-0x40F。应用程序代码和数据可以从 0x410 开始。请参见 Kinetis 120MHz 裸机示例代码中的 vectors.c 和 vectors.h 文件。http://www.nxp.com.cn 上提供了 zip 文件，其中包含如何执行此操作的软件示例。

2.1.3 在启用安全功能后，如何禁用该功能

有多种方法可以禁用安全功能；但请注意，非安全状态选项会受到已编程到闪存配置区段中的闪存安全选项的影响。因此，根据 FSEC 寄存器的当前状态，这些选项可能不可用。

注意

由于 FSEC 寄存器是从闪存配置区段初始化的，因此关闭闪存安全功能的所有方法都是临时的。一旦关闭了安全功能，它将会保持关闭状态，直到下一次复位。必须修改闪存配置区段才能更改安全设置。只要闪存配置区段不再被修改，这些设置将在下一次复位以及此后的每次复位后生效。

2.1.3.1 通过调试器/JTAG 进行大规模擦除

当处理器处于安全状态时，调试器和 JTAG 工具对器件的访问非常有限，唯一可以通过 JTAG 访问的寄存器是 MDM-AP 状态和控制寄存器。为了允许调试工具解除部件的安全状态，可以设置 MDM-AP 控制寄存器的 0 位，以请求对处理器进行大规模擦除。要使用这种方法关闭安全功能，就必须将 FSEC[MEEN] 设置为 10 以外的值，以允许大规模擦除功能。如果禁用了大规模擦除（FSEC[MEEN] = 10），则闪存将忽略大规模擦除请求，因此使用此方法无法解除器件的安全状态。

许多调试器在尝试与器件建立连接时，会自动使用 MDM-AP 状态寄存器的第 2 位来确定器件是否处于安全状态。调试器弹出窗口可用于警告器件已处于安全状态，并询问是否需要进行大规模擦除以解除器件的安全状态。一旦完成大规模擦除并验证后，安全功能将被关闭。某些调试器可能会在大规模擦除完成后，自动对闪存配置区段进行编程，从而将闪存置于非安全状态，FSEC = 0xFE。

2.1.3.2 通过 EzPort 进行大规模擦除

EzPort 也能够使用批量擦除命令（BE）请求大规模擦除以解除器件的安全状态。与通过调试器或 JTAG 进行的大规模擦除一样，必须配置 FSEC 寄存器以启用大规模擦除功能。当完成大规模擦除并验证后，安全功能将关闭。此时，EzPort 可用于使用一个包括所需的闪存配置区段值的新映像对闪存进行编程。

2.1.3.3 使用后门密钥关闭安全功能

如果启用了后门密钥功能，并在闪存配置区段中配置了有效的后门密钥，则可以使用“使用后门密钥解锁安全功能”中描述的后门密钥输入序列来临时关闭安全功能。与用于禁用安全功能的大规模擦除选项不同，如果使用该选项，闪存内容将完全不受影响。由于闪存未被修改，因此闪存配置区段也不会改变。安全功能只是暂时被关闭（除非重新编程闪存配置）。此时，可以自由地读写闪存中存储的代码和数据。

2.1.3.4 使用固件重新编程闪存安全区段

正如“启用安全功能对闪存的影响”一节所述，已编程到闪存中的固件可用于擦除和编程闪存。这包括使用固件命令擦除闪存配置区段，然后将其重新编程的可能性。该方法比较特殊，因为直接对闪存配置区段进行重新编程不会改变 FSEC 寄存器的当前值。因此，如果使用此方法将闪存配置区段重新编程为解除部件安全状态的值，则在处理器复位并将闪存配置区段中的新值载入到 FSEC 寄存器之后，更改才会实际生效。

注意

在大多数 Kinetis 器件上，闪存配置区段位于闪存的第一个扇区。因此，为了擦除闪存配置区段并对其重新编程，需要擦除包括初始栈指针和 PC 值在内的整个矢量表。如果发生断电或固件未正确更新所有的已擦除掉的值，则很可能需要对整个器件进行大规模擦除。

2.1.4 安全和闪存互换功能

具有两个或更多程序闪存（P-Flash）存储块的 Kinetis 器件具有 P-Flash 互换功能。闪存互换功能允许系统编程人员配置 P-Flash 空间的逻辑内存映射，以便两个物理 P-Flash 块中的任何一个都可以存在于相对地址 0x0000 处。互换两个 P-Flash 块的基地址允许系统从 P-Flash 块 0 或 P-Flash 块 1 启动，因为其中任何一块都可以位于基地址 0x0000 处。

要互换闪存块以启动一个备用的应用程序映像，还需要在两个闪存块中都有有效的闪存配置区段。闪存寄存器总是从地址 0x400-0x40F 处加载，因此地址 0x400-0x40F（闪存配置区段）的两个可能选项都必须配置为所需的选项，这一点非常重要。通常，两个闪存块应使用相同的闪存配置区段值。但是，用户可以使用不同的闪存配置区段的设置对两个闪存块进行编程，并使用互换作为一种更改安全和/或保护设置的方法。

3 闪存保护

闪存保护功能用于防止对闪存区域的意外擦除或编程。安全选项可防止外部对微控制器进行未经授权的访问，而闪存保护则可防止对闪存进行写入。当闪存的某个区域受到保护时，则不允许对其内容进行修改。这包括所有的写入访问，甚至包括处理器内部运行的固件请求的写入访问。

闪存保护有多种应用，常见的用例有以下几种：

- 保护闪存中所有包含代码的区域，以防止应用程序本身被覆盖。用于存储数据的闪存区域将不受保护。
- 保护驻留在闪存中的矢量表和引导加载应用程序，而不保护闪存的其余部分。这将防止引导加载程序被意外擦除，但闪存的其他部分不受保护，从而允许引导加载程序执行固件更新。

3.1 闪存保护区域

这些保护功能适用于所有闪存区域：P-Flash、D-Flash，甚至 EEPROM。闪存保护区域的数量和大小根据闪存的类型和闪存块的大小而不同。

3.1.1 P-Flash

对于 P-Flash，总是有 32 个保护区域，它们由 FPROT0–FPROT3 寄存器控制。保护区域的大小为：

（P-Flash 总大小）/32。

表 5 所示为 Kinetis 系列目前可用的基于 P-Flash 总大小的闪存保护区域大小。

表 5. Kinetis P-Flash 保护区域大小

P-Flash 总大小	P-Flash 保护区域大小
1 MB	32
512 KB	16
256 KB	8
128 KB	4
64 KB	2
32 KB	1

3.1.2 D-Flash

对于包含 FlexNVM 的器件，D-Flash 保护由 FDPROT 寄存器控制，其中 D-Flash 大小等于 FlexNVM 的总大小减去用于备份增强型 EEPROM (EEE) 数据的 E-Flash 的大小。由于支持 EEE 功能的 FlexNVM 分区选项可能会导致一些闪存大小不是 2 的幂，因此需要考虑一些特殊情况来确定闪存保护区域的大小。

- 如果 D-Flash 大小是 2 的幂，那么就有 8 个大小相等的保护区域。因此，D-Flash 保护区域的大小由下式给出：

  （D- Flash 总大小）/8

例如，在使用带有 256 KB FlexNVM 的器件时，其中一半的 FlexNVM 用作 D-Flash，另一半用作 EEE 备份（E-Flash），则将有 8 个保护区域，每个区域的大小为 16 KB（128/8 = 16）。

- 如果 D-Flash 的大小不是 2 的幂，那么保护区域的大小就是固定的，实际使用的保护区域将少于 8 个。保护区域的固定大小会根据所使用的特定 Kinetis 器件而不同。具体请参见 http://www.nxp.com.cn 上的特定 Kinetis 参考手册，以获取所对应处理器的正确值。例如，当使用带有 256 KB FlexNVM 的 100 MHz Kinetis 器件时，其中 192 KB 用作 D-Flash（64 KB 用作 EEE 备份），则数据闪存保护区域的大小将为 32 KB。在这种情况下，将只使用 6 个保护区域，而不是 8 个保护区域（32 x 6 = 192），因此 FDPROT[7:6] 必须始终设置为 1，但只有 FDPROT[5:0] 有效。

3.1.3 E-Flash

对于具有 FlexNVM 且使用 EEE 功能的器件，总是有 8 个由 FEPROT 寄存器控制的 EEE 数据保护区域。保护区域的大小将等于 EEPROM 的总大小除以 8。

3.2 配置闪存保护的设置

与安全选项一样，所有的闪存保护寄存器（FPROT0-FPROT3、FDPROT 和 FEPROT）的默认值都是由应用程序映像根据编程到闪存配置区段中的值来确定的。在复位过程中，闪存保护寄存器将载入闪存配置区段中的值。有关不同闪存配置区段地址及与其对应的闪存保护寄存器的说明，请参见表 4。

3.3 更改闪存保护的设置

以下各节将介绍可用于更改闪存保护设置的方法。

3.3.1 大规模擦除

不管调试还是 EzPort 的大规模擦除命令都会忽略闪存保护设置，因此只要 FSEC 设置启用了大规模擦除，就可以使用规模擦除命令，以使芯片返回到没有闪存受到保护的默认状态。

注意

闪存“擦除所有块（Erase All Block）”命令会检查闪存保护设置。如果检查到有任何闪存区域受到保护，则该命令将不会执行。因此，要使用大规模擦除来清除保护设置，就必须使用 JTAG/调试器或 EzPort 等方法。

3.3.2 重新编程闪存配置区段

只要包含闪存配置区段的 P-flash 区域不受保护，就可以使用固件或调试器对该区段进行重新编程（调试器选项仅在器件处于非安全状态下可用）。这种方法可以更改闪存保护位的默认设置。因此，闪存保护位的值可以不受限制地改变，即状态可以从受保护状态切换到不受保护状态。由于更改针对的是保护寄存器的默认状态，而不是寄存器本身，因此所做的任何更改都只在下一次复位后才会生效。

注意

在大多数 Kinetis 器件上，闪存配置区段位于闪存的第一个扇区。因此，为了擦除和重新编程闪存配置区段，需要擦除包括初始栈指针和 PC 值的整个向量表。

注意

请注意，包含闪存配置区段的闪存区域可以受到保护。如果闪存配置区段受到保护，用户将无法擦除闪存配置区段，以及进一步对其重新编程以更改保护设置。因此，建议在使用闪存保护和启用安全功能时，保留启用大规模擦除功能。

3.3.3 写入保护寄存器

与 FSEC 寄存器不同，直接写入闪存保护寄存器是允许的，但只能用于加强保护。不允许写入闪存保护寄存器以解除对某一区域的保护。闪存实际上允许在 NVM 特殊模式下执行此操作，但 SoC 并不使用 NVM 特殊模式，除非部件处于 EzPort 模式。此外，这些更改只持续到下一次复位之前。如果芯片经历了一次复位，则寄存器将从闪存配置区段重新载入，因此在那时，任何对保护寄存器的直接更改都将丢失。

4 篡改检测和加密

一些 Kinetis 系列器件提供篡改检测（DryIce 模块）和/或加密功能（CAU 和 RNG 模块）。对这些功能的详细讨论超出了本应用笔记的范围，但有计划在其他应用笔记讨论这些模块。详情请访问 http://www.nxp.com.cn/kinetis 查看最新的应用笔记。篡改检测和加密功能是对安全和保护功能的实用补充，在规划整体安全策略时必须加以考虑。

CAU 可用于加密/解密芯片上的任何外部接口的数据。本应用笔记中介绍的安全功能有助于确保处理器内部信息的安全，但该加密模块可用于保护和确保传到或传自于外部设备或通信端口的数据的完整性。DryIce 模块包括篡改检测信号，可用于确定是否有人试图干扰 PCB 上的隔离区和/或电路以访问系统。

How to Reach Us:

Home Page:
www.nxp.com.cn

Web Support:
http://www.nxp.com.cn/support

USA/Europe or Locations Not Listed:
NXP Semiconductor
Technical Information Center, EL516
2100 East Elliot Road
Tempe, Arizona 85284
+1-800-521-6274 or +1-480-768-2130
www.nxp.com/support

Europe, Middle East, and Africa:
NXP Halbleiter Deutschland GmbH
Technical Information Center
Schatzbogen 7
81829 Muenchen, Germany
+44 1296 380 456 (English)
+46 8 52200080 (English)
+49 89 92103 559 (German)
+33 1 69 35 48 48 (French)
www.nxp.com/support

Japan:
NXP Semiconductor Japan Ltd.
Headquarters
ARCO Tower 15F
1-8-1, Shimo-Meguro, Meguro-ku,
Tokyo 153-0064
Japan
0120 191014 or +81 3 5437 9125
support.japan@nxp.com

Asia/Pacific:
NXP Semiconductor China Ltd.
Exchange Building 23F
No. 118 Jianguo Road
Chaoyang District
Beijing 100022
China
+86 10 5879 8000
support.asia@nxp.com

Document Number: AN4507
Rev. 1, 6/2012