freescale™
飞思卡尔

Kinetis MCU

为未来的互联网保驾护航

freescale.com/Security

Kinetis 微控制器

安全、可扩展、超低功耗、混合信号MCU

Kinetis 微控制器 (MCU) 包含多个系列的硬件和软件兼容的ARM® Cortex®-M0+ 和M4 MCU产品，并规划了令人兴奋的新路线图，新的Cortex-M7内核已经列入计划。Kinetis MCU系列包含近1000款MCU，是目前最广泛、基于ARM的MCU产品组合，具有卓越的低功耗性能、可扩展性与功能集成，提供多种通用或针对特定应用的功能。

超级可扩展

有近1000款Kinetis MCU型号，可以提供非常多样的选择和无与伦比的可扩展性能，拥有多达2 MB的闪存和256 KB的SRAM，且软件和硬件兼容，能够极大地保护您的工程投资。

优化配置

片上集成的多种智能选项，包括HMI、安全、混合信号功能和连接选项，例如带无晶体功能的USB，帮助客户降低总物料成本。

性能和能效

体验带浮点单元的180MHz最佳性能，享受多个低功耗模式和增强型节能外设实现的长电池寿命。

全方位支持

使用飞思卡尔及其他ARM生态合作体系供应商提供的广泛的软件和工具套件加快应用开发。

安全性

充分利用整个Kinetis MCU产品组合共享的安全架构，提供一系列解决方案，无论是简单的边缘节点，还是先进的支付解决方案。

安全和完整的解决方案

以下几页介绍了Kinetis MCU的各种安全模块。请注意Kinetis MCU包含许多资源，可用于创建安全的嵌入式应用。广泛的器件组合提供多种存储器和性能，还包含安全外设选项，以满足不同的应用需求。从固件保护机制到用于先进的加密密钥管理的防入侵硬件，Kinetis MCU安全架构是您下一个安全设计的关键要素。

Kinetis MCU安全架构的特点和优势

特性	优势	特性详细信息	支持	产品
片上闪存的安全性和保护机制	防止固件被盗和应用克隆	• 能够阻止通过调试接口访问处理器 • 能够设置64位密钥，重新获得调试访问	AN4507：使用Kinetis的安全特性和闪存保护功能	所有Kinetis器件
调试端口配置	阻止外部的调试请求或闪存的重新编程	能够通过软件控制禁用JTAG		
唯一ID	通过软件将MCU唯一地识别为可信任器件	• 128位唯一ID（Kinetis K系列MCU） • 80位唯一ID（Kinetis L系列MCU） • 64位唯一ID（Kinetis E系列MCU）		
只从内部存储器启动	受控启动条件可避免使用外部存储器进行的攻击	NVM控制位用于设置启动条件		
使用引导ROM进行加密固件升级	利用内置ROM例程保护固件更新，降低软件开支和复杂性	• 固件通过AES128位密钥进行加密 • 完全支持内部闪存安全性，包括通过预设密钥批量删除或解除安全的功能 • 执行引导程序有多种方案，或在系统启动时，或在运行时通过应用控制。配置QuadSPI接口的功能，取决于外置QuadSPI内的配置信息。		在Kinetis K80_150, K81_150, K82_150 MCU中部署
片外存储器访问控制，适用于SDRAM和FlexBus的并行存储器	受控的程序执行条件，用于避免使用外部存储器进行的攻击	FlexBus安全性选项，决定是否能从外部存储器执行		所有带FlexBus外设的Kinetis MCU
存储器保护单元 (MPU) 监控系统总线的操作	系统监控程序的执行，确保程序是在预期的存储器范围内运行，赋予运行软件有限的访问权限。	MPU使用预先配置的访问区域描述符监控总线操作的合法性，访问区域描述符定义了存储空间和相应的访问权限。		在Kinetis K80_150, K81_150, K82_150, K70_120, K63_120, K64 _120, K60_120, K53_100, K24_120, K21_120, K21_ 50, K11_50 MCU中部署
闪存访问控制 (FAC) 可配置存储器保护机制，允许用户使用软件库，同时为这些库提供可编程限制。	保护软件IP	借助非易失性控制寄存器设置对片上闪存资源的访问权限。可对64个不同的分段设置管理权限或仅执行访问权限	AN5211：使用Kinetis闪存仅执行访问控制的功能	在Kinetis K22_100, K26_180, K66_180, K65_180, K80_150, K81_150, K82_150 MCU中部署
用于加速对称加密和哈希函数的硬件和软件机制	为加密功能降低CPU负载。提供对数据篡改侦测的手段。简化更高级安全功能及网络安全标准的实施。针对固件更新，可将固件散列与加密密钥结合使用，确保正在更新的固件是可信固件。	采用硬件实现对称加密安全运算， 支持DES、3DES、AES、MD5、SHA-1和SHA-256 算法	AN4307：使用Kinetis MCU中的mmCAU	在Kinetis K80_150, K81_150, K82_150, K70_120, K63_120, K64 _120, K60_120, K53_100, K24_120, K21_120, K21_ 50, K11_50 MCU中部署
LTC：面向AES、 DES和公钥加密的加密协处理器	分流CPU负载，减少软件占用空间。加速RSA2048、ECDSA和ECDH，减少认证延迟	LTC集成了多个加密硬件加速引擎，这些引擎共享通用寄存器。该LTC版本支持AES、DES、3DES、RSA和ECC。	Kinetis SDK驱动程序	在Kinetis K81_150，K82_150 MCU中部署
从外部串行NOR闪存进行动态AES解密	保护片外固件的安全	硬件模块对QuadSPI提取的外部闪存数据进行AES128计数器模式解密，支持软件在芯片内执行，不会增加延迟		在Kinetis K81_150，K82_150 MCU中部署
入侵检测模块带8个入侵侦测引脚	减少防入侵机制所需的外部电路	在发生外部攻击事件时，可通过异步删除操作保护密钥存储空间。检测引脚、温度、电压和时钟等间接攻击，以及主动的攻击	可为签署NDA的客户提供应用说明	在Kinetis K81_150, K70_120, K61_120, K63_120, K21_120, K21_ 50, K11_50 MCU中部署
安全会话RAM	带安全功能的暂时存储器	RAM内存块用于存储敏感信息（如加密会话密钥），当检测到入侵事件时，会自动删除这些敏感信息		在Kinetis K81_150 MCU中部署

硬件加密

概述

硬件加密协处理器为开发人员提供了数据的传输和存储安全。它支持用硬件实现一组专门运算，提高基于软件的加密/解密过程的吞吐量以及改善消息摘要功能。

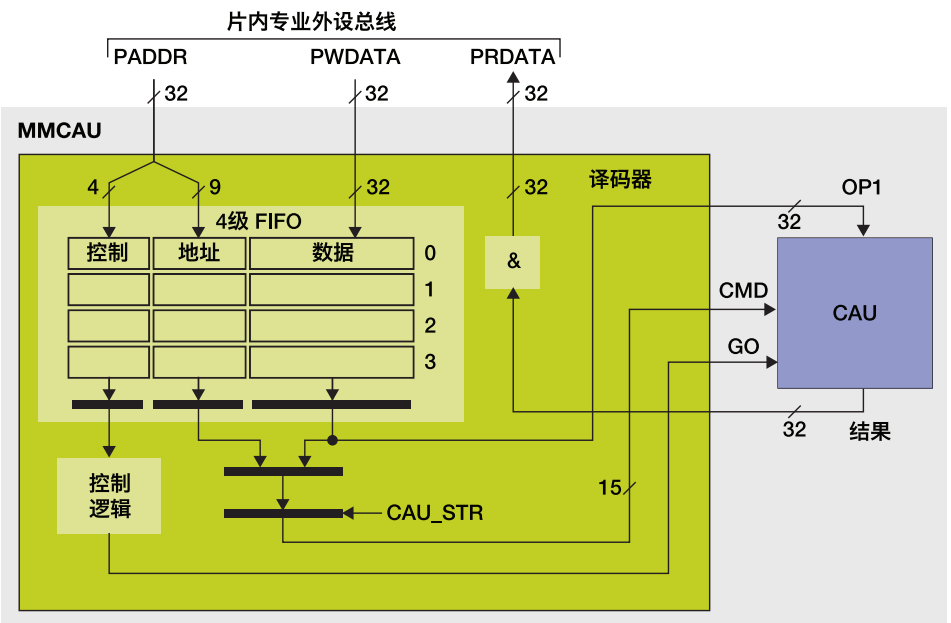
特性

- 支持加密及数据哈希运算所需的最常用函数，包括DES、3DES、AES、MD5、SHA-1和SHA-256算法
- 能够在一次数据写入操作中发送3个命令，提高软件算法之外的吞吐量
- 使用协处理器指令实现安全函数的最核心部分，免费提供对应的软件库
- 借助标准的处理器指令实施更高级的软件功能
- 完美支持各种网络安全标准 (SSL、IPsec)
- 允许实施任何高级的功能或操作模式 (HMAC、CBC等)

飞思卡尔以应用笔记的方式提供免费的加密软件示例：

CAUAP：加密加速单元：CAU和mmCAU软件库

MMCAU框图



mmCAU内置模块

项目	描述
译码器子模块	提供片内专用APB接口与CAU模块之间的桥梁。将APB上的存储器映射命令和数据传输给CAU，或从CAU取出。
四级FIFO	包含命令和输入操作数，以及从PPB捕捉的和发送给CAU的相关控制
CAU	三个终端模块，带命令和（可选）输入操作数及结果总线

外部看门狗监视器（EWM）

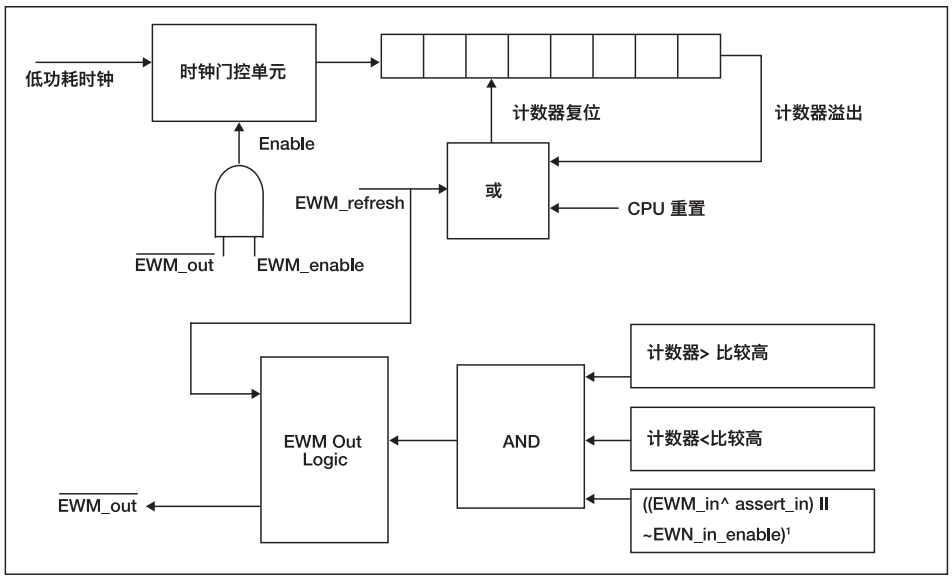
概述

看门狗用于监控MCU嵌入式软件的流程和执行情况。外部看门狗监视器旨在作为冗余看门狗系统，监测外部电路以及MCU软件流程。这样就提供了内置看门狗的备份机制，实现复位MCU的CPU和外设。

特性

- 独立的LPO时钟源提供可靠的集成时钟源
- 根据EWM LPO时钟周期数指定的可编程超时时间，为与广泛的外部选件配合提供灵活性
- 窗口式刷新选项
- 在被触发后，一个输出端口可以用于复位或将外部电路设置于安全模式
- 一个输入端口允许外部电路控制输出端口信号
- 在等待、停止和调试模式下工作

外部看门狗框图



[1]比较高 > 计数器 > 比较低

存储器保护单元

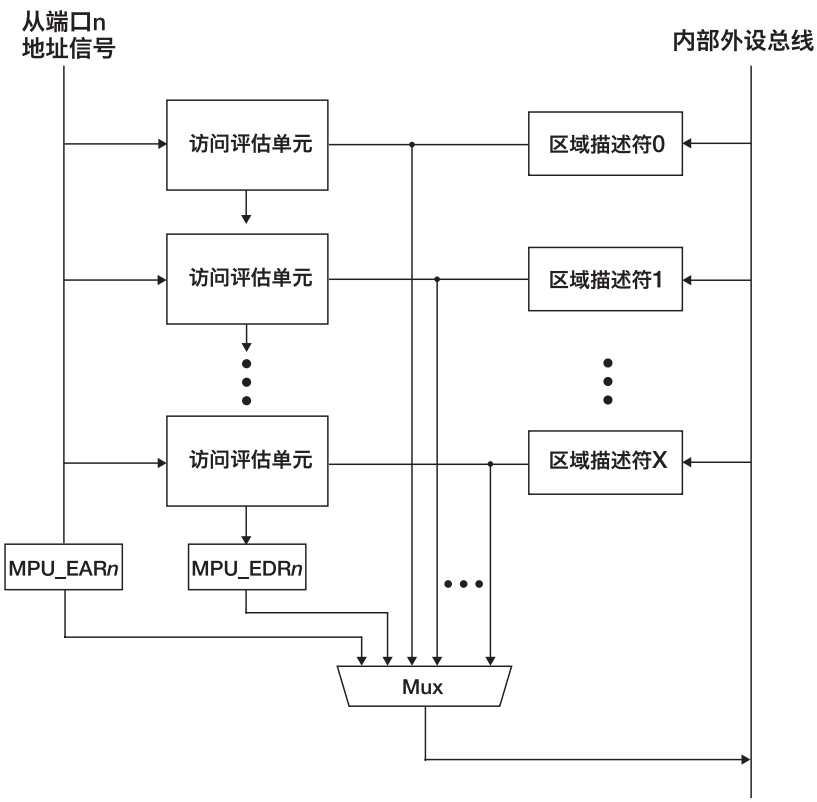
概述

该存储器保护单元监控系统总线的传输，并使用预先配置的访问区域描述符监控总线操作的合法性，访问区域描述符定义了存储空间和相应的访问权限。仅允许具有足够访问权限的存储器操作请求，拒绝对未映射到任何区域描述符的存储空间的操作，并返回保护错误响应。

特性

- 多达16个程序可见的，128位区域描述符可提供最大的灵活性，支持多层访问控制的软件管理。
- 可设置读、写、执行属性。
- 借助描述符有效位的硬件辅助维护，可最大限度地减少一致性问题。
- 如果内存操作区间与任何内存区域都不匹配或者在所有匹配的内存区域内操作都是非法的，则会检测到存取保护错误。如发生存取错误，则操作会被终止并返回错误响应，存储器保护单元将禁止对目标从设备的总线操作。
- 错误寄存器（每个从端口）捕捉上次发生错误的地址、属性和其他信息，实现故障可追溯性。
- 全局存储器保护单元启用/禁用控制位可实现轻松控制。

存储器保护单元框图



入侵检测

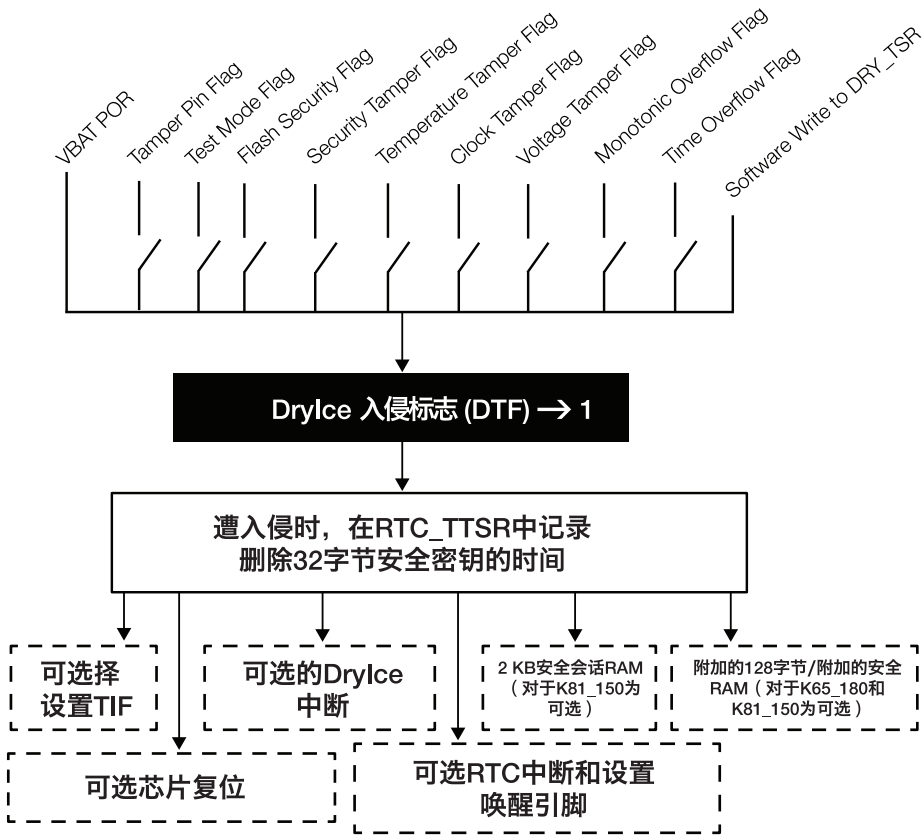
概述

入侵检测模块提供安全密钥存储，带有针对不安全闪存、温度、时钟、电源电压变化的内部/外部入侵的检测功能，以及物理攻击检测。

特性

- 独立的电源、POR（上电复位）和32 KHz振荡器
- 32字节的安全存储、当检测到入侵时复位
- 入侵时间寄存器记录检测到的入侵时间
- 两个主动入侵移位寄存器，每个寄存器都带有可配置的多项式
- 寄存器保护
- 多达10个内部入侵检测源，包括时间计数器溢出、电压、温度和时钟超出范围、闪存安全禁用和进入测试模式，以及可选的DryIce和安全模块
- 多达8个外部入侵检测引脚，能够产生中断或入侵事件
- 可配置的极性和数字尖峰滤波器，具有可选的预分频器
- 可针对静态或主动入侵输入进行配置
- 支持软件发起的入侵引脚设置

DryIce入侵检测模块



随机数发生器

概述

Kinetis MCU可配备两种随机数发生器。第一种是**随机数发生器加速器**，它是能够生成32位随机数的数字集成电路。

- 通过环形振荡器为移位寄存器提供时钟，生成随机位。
- 移位寄存器的配置确保良好的数据统计。
- 振荡器的频率未知，可提供创建随机数据所需的熵。

强烈建议将该模块产生的随机数据作为种子输入到NIST批准的伪随机数生成器。

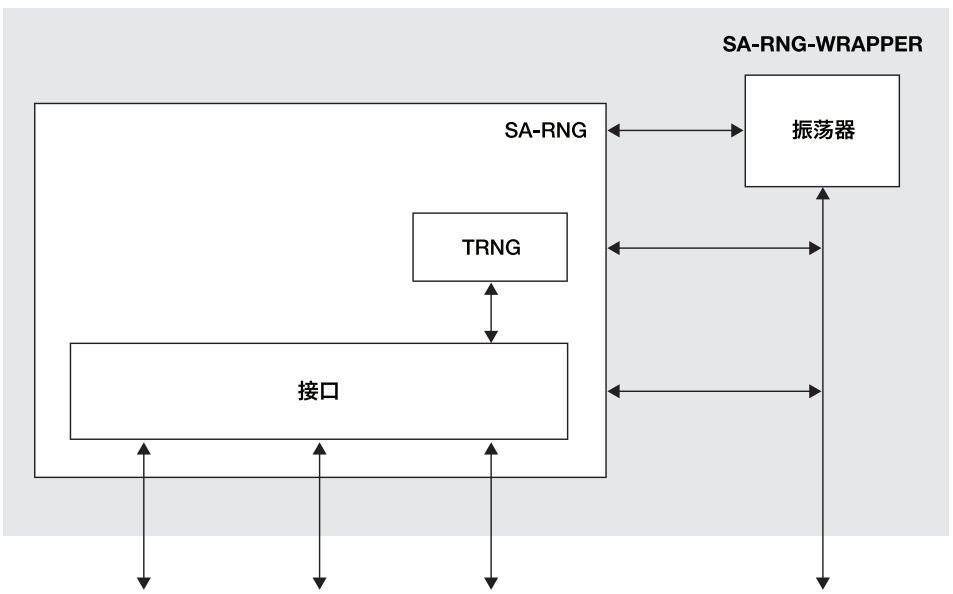
Kinetis K8x MCU系列可用的第二种随机数发生器是**独立的真随机数发生器**（或SA-TRNG）。SA-TRNG是硬件加速器模块，可根据熵接收模块或其他后处理功能的需要生成512位的熵。

TRNG生成的熵被直接用于生成密钥的函数、基于消息密钥的函数、随机质询函数，以及加密算法使用的其他相关量。

TRNG的基本原理是从随机噪声源收集比特。随机噪声源是一个环形振荡器，它对使用TRNG的器件内的随机噪声（温度变化、电压变化、串音和其他随机噪声）非常敏感。

TRNG可用于为由硬件或软件实现SP800-90所定义的DRBG算法提供种子。

独立的真随机数生成器 (SA-TRNG)



LP可信加密 (LTC)

概述

LP可信加密集成了多个加密硬件加速引擎，这些引擎共享通用寄存器。该LTC版本支持AES、DES、3DES、RSA和ECC。

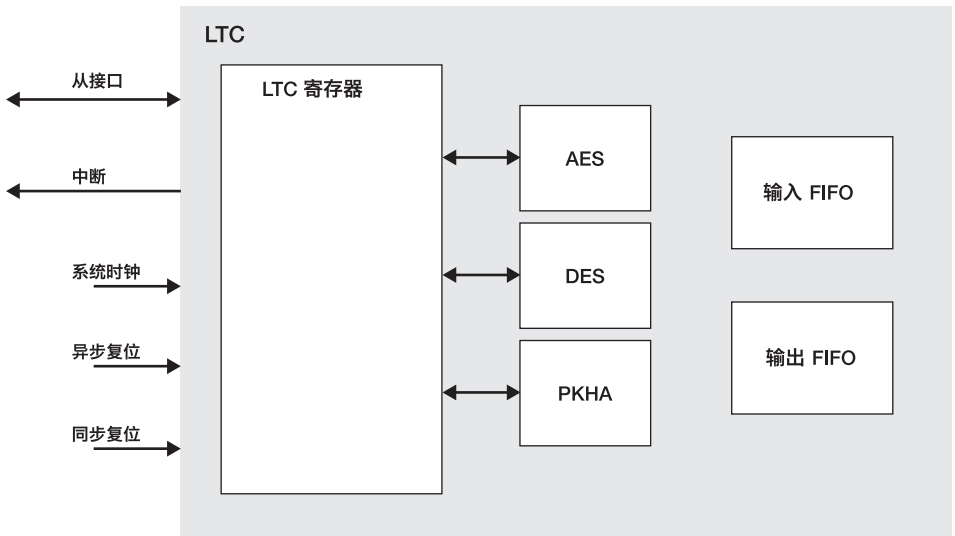
特性

- 支持AES128和AES256，还支持:
  - 保密 (ECB、CBC、CTR、OFB、CFB128)
  - 认证保密 (CCM)
  - 认证 (XCBC-MAC, CMAC)
- DES功能和3DES功能，以及ECB、CBC、CFB和OFB模式和密钥奇偶校验，以上都符合DES规范。
- 公钥硬件加速器，能够执行公钥加密中所用的多种不同运算，包括模运算函数，如加、减、乘、求幂、简约和模反，以及点法、倍点和点乘等椭圆曲线函数。

软件支持

- Kinetis SDK提供LTC驱动程序
  - 支持对称模式和非对称模式
  - 支持公钥密码
    - RSA, ECDSA, ECDH

LP可信加密 (LTC) 框图

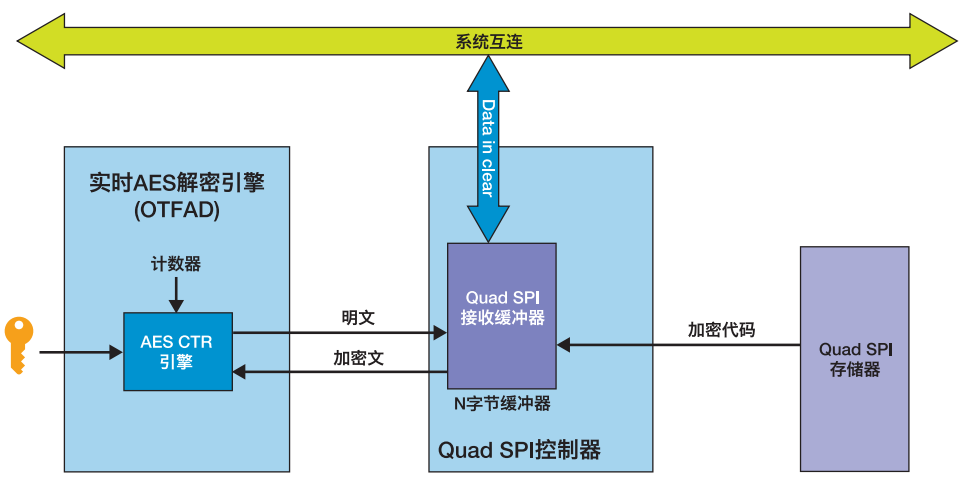


实时AES解密模块 (OTFAD)

特性

- 实时解密模块与QuadSPI的外部闪存控制器相结合，支持与加密的外部串行NOR闪存对接。
- QuadSPI以及内置的高速缓存存储器，得到的综合存取速度，允许直接从外部存储器执行应用代码，无需将代码复制到另一个（速度更快的）存储器中。
- OTFAD引擎采用运算块加密模式，专门支持计数器模式 (CTR) 。
- OTFAD引擎将解密后的数据传送回QuadSPI接收缓冲器，提供给内部系统。
- 为4个独立的解密部分提供硬件支持，称为内存上下文。
  - 每个上下文都拥有唯一的128位密钥、64位计数器和64位内存区域描述符。

实时AES解密模块 (OTFAD) 框图



资源

产品页

freescale.com/Kinetis/Kseries:

- Kinetis K8x MCU系列
- Kinetis K7x MCU系列
- Kinetis K6x MCU系列
- Kinetis K2x MCU系列
- Kinetis K1x MCU系列

飞思卡尔Freedom开发平台

freescale.com/Freedom

塔式系统模块化开发平台

freescale.com/Tower

Kinetis MCU软件开发套件

freescale.com/KSDK

免费赠送的USB协议栈，带个人医疗保健设备和USB音频等级

freescale.com/USB

传感器融合解决方案

http://www.freescale.com/sensorfusion

飞思卡尔Touch软件

www.freescale.com/TouchSW

freescale™ 飞思卡尔

如需了解更多信息，请访问 freescale.com/Security

文档编号：BRKINETISSECSOLS REV 2