AN13198

OTFAD 在 i.MXRT1170 上的性能表现

第 0 版 — 2021年5月19日 应用笔记

目录

1 简介

1.1 目的

本应用笔记的目的是比较未加密时和使用OTFAD模块解密时外部闪存的读取速度。

1.2 目标读者

本文档适用于那些需要全面了解OTFAD解密性能的人。它没有介绍如何创建加密的XIP OTFAD镜像文件。它假定读者已经熟悉i.MX RT1170上的OTFAD模块提供的加密XIP的基础知识。它还假定读者已经熟悉SPT安全配置工具。

1.3 范围

本文档是一个实际的示例，提供了未加密XIP与加密XIP读取性能相比较的测量结果。

1.4 首字母缩略词和缩写

本文件中使用的术语和首字母缩写为：

- AES – 高级加密标准。
- AHB – 连接到FlexSPI模块的内部总线。
- AXI – 连接到一级缓存的内部总线。AXI和AHB与AHB/AXI总线转换器相连。
- FlexSPI – NXP专有模块，用于访问单/双/四/八线/Hyperbus和类似的基于串行总线的设备。
- XIP – 就地执行。它是指直接从非易失性存储器执行软件映像。
- Unencrypted XIP – 指直接从非易失性存储器执行软件映像，无需使用任何解密。
- Normal XIP – 指未加密的XIP。
- Encrypted XIP – 指直接从非易失性存储器执行加密软件映像，必须由OTFAD模块进行解密。
- OTFAD – 即时AES解密模块。
- SPT – 安全配置工具，提供加密的XIP映像，并将映像上载到目标板。
- MCUX IDE – MCUXpresso IDE。它是一个易于使用的集成开发环境（IDE），用于创建、构建、调试和优化应用程序代码。
- ITCM – 通过其自身的I-TCM总线接口访问的内部存储器（建议用于进行指令提取的单周期存储器-代码执行，中断向量表等）。

- DTCM – 通过其自身的D0-TCM/D1-TCM接口访问的内部存储器（建议用于进行数据访问单周期存储器-堆栈、重要静态变量等）。
- I-CACHE
  - 读缓存命中：代表用于指令获取的单周期内存。
  - 读缓存未命中：在AXI总线上生成32-B突发传输。
- D-CACHE
  - 读缓存命中：代表数据访问的单周期内存。
  - 读缓存未命中：在AXI总线上生成32-B突发传输。
- OCRAM – 通过互连总线结构NIC由AXI总线访问的内部存储器。它应被缓存以达到足够的性能。通过AXI访问时会生成多个等待状态。数据由多个主机访问，如CM7和DMA。如果可能，避免在此处放置堆栈。

2 OTFAD 模块

即时AES解密（OTFAD）模块提供了一种先进的硬件实现方式，可以最大限度地减少在整体外部存储器访问时间中由解密引入的延迟的增加周期。它实现了一种支持计数器模式（CTR）的分组密码操作模式。CTR模式提供了一种保密模式，其特点是对一组输入块（称为计数器）应用前向密码，产生一系列输出块，这些输出块与明文异或以产生密文，反之亦然。

OTFAD引擎包括对标准AES密钥展开机制的完整硬件支持，用于解密密钥BLOB数据指令，其中包含多达4个独立的AES上下文所需的参数。每个上下文都含一个唯一的128位密钥、一个64位计数器和一个64位存储区域描述符。

2.1 OTFAD 模块的基本功能

- AES-128计数器模式即时解密。
  - 128位密钥和128位数据块大小。
  - 128位计数器包括64位初始化向量加上32位系统地址。
- 当与FlexSPI一起使用时，它对于解密所增加的延迟周期为零。
  - 它从FlexSPI接收64位加密数据，计算解密数据，将其发送到AHB RAM缓冲区，并绕回系统AHB读取数据总线。
- 硬件支持4个独立的解密段（称为存储器“上下文”）。
  - 每个上下文都含一个唯一的128位密钥、一个64位计数器和一个64位存储区域描述符。
- 它在功能上充当FlexSPI的从属子模块。
  - 它在FlexSPI及其AHB RAM缓冲区之间进行逻辑连接。
  - 它共享系统AHB和IPS（从外围设备）的总线连接。
  - 编程模型被映射到FlexSPI的IPS地址空间的高1K字节。
  - 用于加密（密文）和解密（明文）数据的专用64位数据总线。
- 硬件微体系结构。
  - 高度流水线化的针对加密进行了优化的AES引擎，每个周期可执行3轮。
  - 64位AHB连接，便于与系统总线结构和FlexSPI进行集成。
  - 针对两个128位加密计数器和三个64位解密数据缓冲区的数据存储。
  - 针对{32,64}位WRAP4突发传输（CPU缓存未命中提取大小和典型的DMA提取大小）进行了优化。

2.2 OTFAD 框图

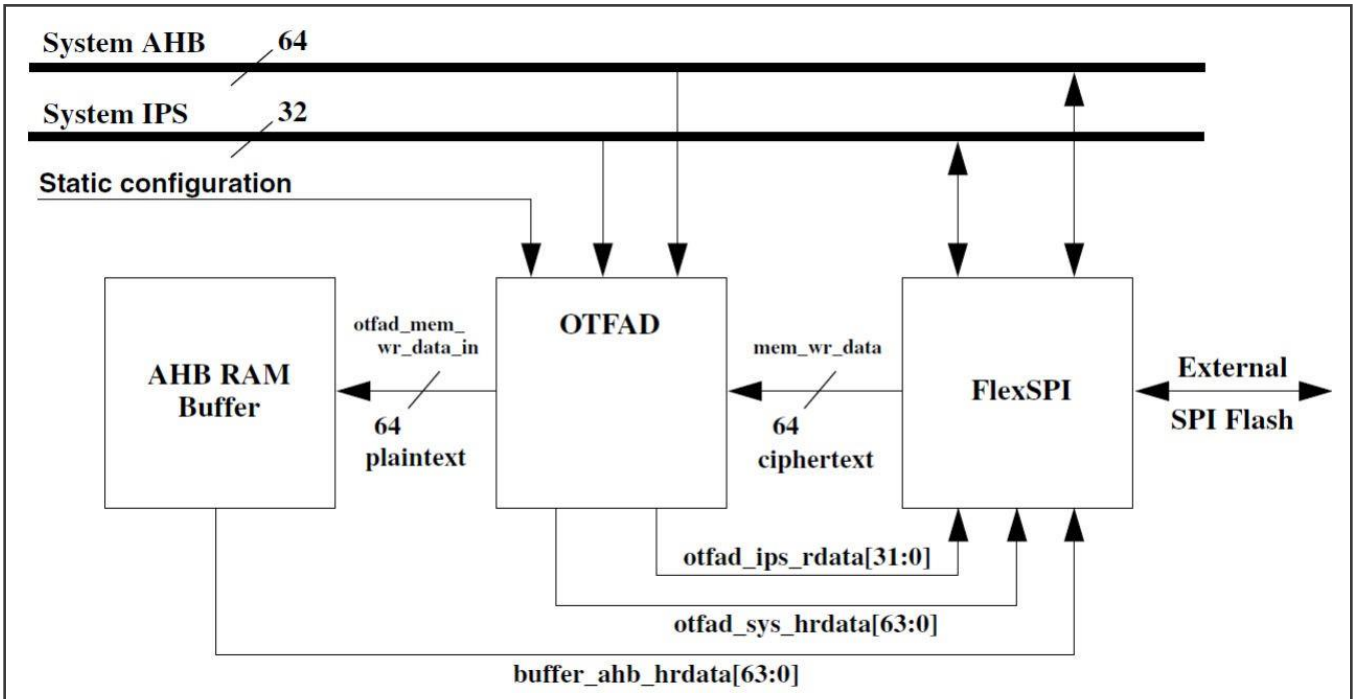

图1. OTFAD和FlexSPI的连接拓扑

2.3 OTFAD 总线定时

这是原始地址为0x00的64位WRAP4读取请求的示例。

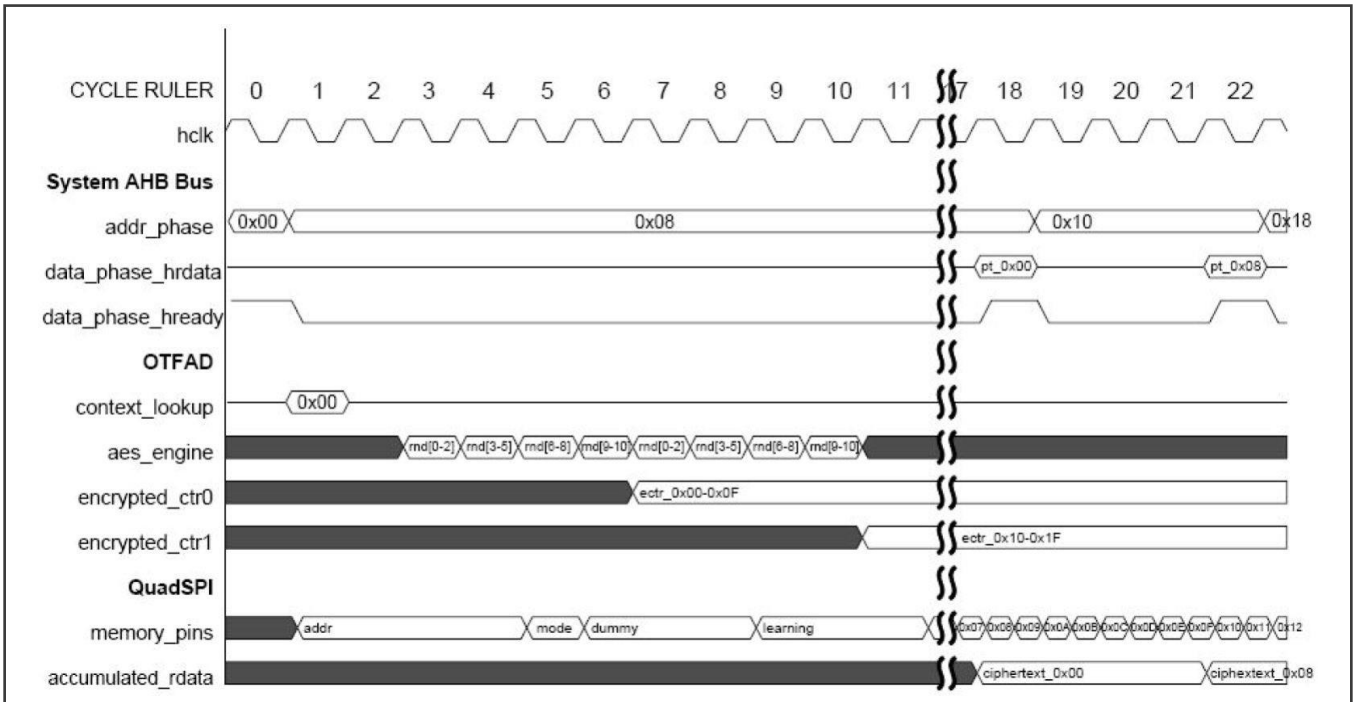

图2. OTFAD 64位WRAP4突发传输时序图

当命令、地址和模式位在FlexSPI总线引脚上传输时，AES引擎会同时准备所有“encrypted_ctr0”和“encrypted_ctr1”值，而当数据从QSPI存储器中读取时，它们也准备好了进行异或操作。这完成了AES-CTR模式的实现，而该模式由OTFAD模块提供。FlexSPI和OTFAD组合的结果可以提供最佳的系统性能。

3 测量

3.1 硬件要求

使用MIMXRT1170-EVK板进行测量。使用FlexSPI1模块端口A，因为默认情况下它被连接到QSPI存储器。

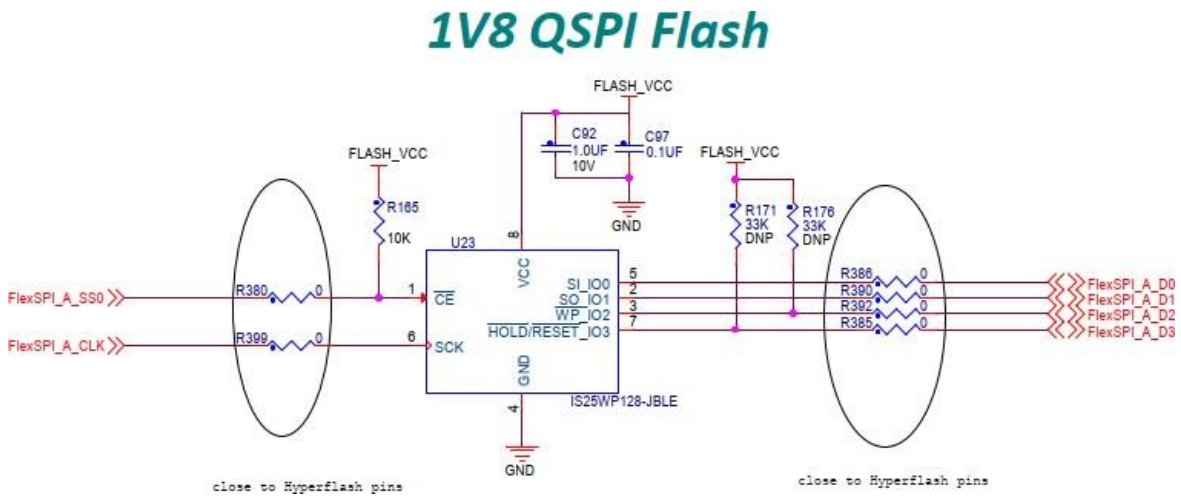

图3. QSPI闪存连接至FlexSPI1端口A

3.2 软件工具

使用的软件如下：

- MCUXpresso IDE v11.3.0 [Build 5222]
- "evkmimxrt1170_flexspi_OTFAD_performance_cm7" 测试应用代码——软件与此文档一同提供
- 加密配置工具v3.1

3.3 测量方法

测量的目的是比较在有和没有OTFAD模块解密的情况下从闪存读取数据的速度。

测量本身由MCUX IDE应用程序“vkmimxrt1170_flexspi_OTFAD_performance_cm7”完成。应用程序代码在只读闪存地址空间中分配两个读缓冲区，并使用CM7内核的周期计数器测量从这些读缓冲区的读取数据的时间。

为了获得这两个结果，测量应用程序的印像文件在第一种情况下作为正常的XIP上传，在第二种情况下作为加密的XIP（OTFAD模式）上传。在这两种情况下，上传的是相同的印像文件。因此，不管是对于普通XIP还是加密XIP，FlexSPI模块都采用的相同设置。只有提供给引导ROM代码的OTFAD设置不同。要创建加密的XIP映像文件并将其上载到目标板，请务必使用安全配置工具（SPT）v3.1。

3.4 测量应用程序

应用程序代码基于SDK的示例代码“evkmimxrt1170_flexspi_nor_polling_transfer_cm7”。

闪存中有两个16-KB的只读缓冲区，其中填充了0–16383的递增值。

```
const uint32_t text_read_buffer1[]_attribute_((aligned(1024))) = { T_FILL4096(0) };
const uint32_t text_read_buffer2[]_attribute_((aligned(1024))) = { T_FILL4096(0) };
```

3.4.1 FlexSPI 模块设置

测试是用1V8 QSPI闪存IS25WP128-JBLE做的。SDK闪存驱动程序使用的FlexSPI设置如下：

- 使用SDR/READ_FAST_QUAD进行默认AHB访问。
- 为内核使能大小为4 KB的预取缓冲区。
- 使能FlexSPI根时钟至99 MHz。

3.4.2 测试函数

- “flexspi_nor_readData_8b_itcm”函数测量采用8位访问模式从“文本读取缓冲区1”读取数据的内核周期数：

```
__ASM volatile ("LDRB.W r3,[r0],#1\n");
__ASM volatile ("LDRB.W r3,[r0],#1\n");
```

- “flexspi_nor_readData_pingpong_8b_itcm”函数测量采用8位访问模式从“文本读取缓冲区1“和”文本读取缓冲区2”交替读取数据的内核周期数：

```
__ASM volatile ("LDRB.W r3,[r0],#1\n");
__ASM volatile ("LDRB.W r3,[r1],#1\n");
```

- “flexspi_nor_readData_16b_itcm”函数测量采用16位访问模式从“文本读取缓冲区1”读取数据的内核周期数：

```
__ASM volatile ("LDRH.W r3,[r0],#2\n");
__ASM volatile ("LDRH.W r3,[r0],#2\n");
```

- “flexspi_或_readData_pingpong_16b_itcm”函数测量采用16位访问模式从“文本读取缓冲区1”和“文本读取缓冲区2”交替读取数据的内核周期数：

```
__ASM volatile ("LDRH.W r3,[r0],#2\n");
__ASM volatile ("LDRH.W r3,[r1],#2\n");
```

- “flexspi_nor_readData_32b_itcm”函数测量采用32位访问模式从“文本读取缓冲区1”读取数据的内核周期数：

```
__ASM volatile ("LDR.W r3,[r0],#4\n");
__ASM volatile ("LDR.W r3,[r0],#4\n");
```

- “flexspi_或_readData_pingpong_32b_itcm”测量采用32位访问模式从“文本读取缓冲区1”和“文本读取缓冲区2”交替读取数据的内核周期数：

```
__ASM volatile ("LDR.W r3,[r0],#4\n");
__ASM volatile ("LDR.W r3,[r1],#4\n");
```

- “flexspi_nor_readData_burst_itcm”函数测量使用突发访问模式从“文本读取缓冲区1”读取数据的内核周期数：

```
__ASM volatile ("LDM r1,{r4-r11}\n");
```

所有这些函数都位于ITCM中并在ITCM中执行，不影响“文本读取缓冲区”的读取速度。

3.4.3 L1 D-CACHE 设置

根据一级D缓存的设置，测量函数采用以下三种方式执行：

1. D-CACHE禁用。在测量之前，缓存被禁用。
2. D-CACHE无效。在每次测量之前，D-CACHE被启用但失效。
3. D-CACHE已满。第一次测量时，D-CACHE被启用并填满测量值。下一次测量时不失效D-CACHE，预计将提供100%的缓存命中率。返回第二次测量的值。

3.4.4 缓冲区大小设置

整个测量是针对分别被设置为4KB和16KB的“文本读取缓冲区1”和“文本读取缓冲区2”进行的。必须根据每个缓冲区大小的设置来构建应用程序。

4 测量结果

Cortex M7 - CORE @[illegible], QSPI @[illegible] SDR								
			4K read buffer			16K read buffer		
			D-CACHE			D-CACHE		
			Disabled	Invalidated	Filled	Disabled	Invalidated	Filled
Standard FlexSPI access	Linear READ	8-bit	18.29	47.64	995.51	18.38	47.73	995.88
		16-bit	36.72	47.71	1990.06	36.74	47.74	1991.51
		32-bit	47.68	47.71	3976.23	47.72	47.75	3982.06
		BURST 8	47.71	47.65	5277.64	47.75	47.73	5303.37
	PingPong READ	8-bit	1.46	25.9	1061.85	1.46	27.03	1062.19
		16-bit	2.91	25.71	2274.03	2.93	26.98	2275.62
		32-bit	5.83	25.82	4710.87	5.89	27.01	4588.99
		BURST 8	-	-	-	-	-	-
OTFAD FlexSPI access	Linear READ	8-bit	19.65	46.93	995.51	19.76	47.01	995.88
		16-bit	39.14	47.01	1990.06	39.16	47.05	1991.51
		32-bit	46.91	47.01	3976.23	46.93	47.05	3982.06
		BURST 8	47.01	46.95	5227.64	47.05	47.03	5303.37
	PingPong READ	8-bit	1.46	27.71	1061.85	1.46	27.73	1062.19
		16-bit	2.93	27.63	2274.03	2.93	27.71	2275.62
		32-bit	5.96	27.63	4710.87	5.96	27.71	4588.99
		BURST 8	-	-	-	-	-	-

图4. 测量的传输速度（以MB/s为单位）

5 结论

结果与将FlexSPI连接到内部64位AHB总线的硬件规格是一致的。最好的结果是采用32字节突发访问模式获得的。当D-CACHE失效时，意味着它不包含任何缓存数据，因此8位或16位访问模式会明显加速。这是因为传入的8位请求会作为32字节请求传输到AXI/AHB总线。缓存中填充了32字节的响应值，接下来的31个8位读取请求会在D_缓存中命中。

最终的结果是，可以通过本应用程序测得，OTFAD模块没有造成任何显著的性能下降。这得益于OTFAD模块的设计和AES128-CTR解密模式的实现。

6 参考资料

1. MXUXpresso IDE - https://www.nxp.com/design/software/development-software/mcuxpresso-software-and-tools-/mcuxpresso-integrated-development-environment-ide:MCUXpresso-IDE
2. Secure Provisioning Tool - https://www.nxp.com/design/software/development-software/mcuxpresso-software-and-tools-/mcuxpresso-secure-provisioning-tool:MCUXPRESSO-SECURE-PROVISIONING?tid=vanMCUXPRESSO-SECURE-PROVISIONING
3. *i.MX RT1170 Processor Reference Manual* (document IMXRT1170RM)
4. *Security Reference Manual for the i.MX RT1170 Processor* (document IMXRT1170SRM)
5. *Using the i.MXRT L1 Cache* (document AN12042)
6. AN memory benchmark performance by RP ***please provide the document ID)***

7 修订历史

表1. 修订历史

版本号	日期	内容变化
0	2021年5月19日	初版发布

How To Reach Us

Home Page:

nxp.com

Web Support:

nxp.com/support

Information in this document is provided solely to enable system and software implementers to use NXP products. There are no express or implied copyright licenses granted hereunder to design or fabricate any integrated circuits based on the information in this document. NXP reserves the right to make changes without further notice to any products herein.

NXP makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does NXP assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. "Typical" parameters that may be provided in NXP data sheets and/or specifications can and do vary in different applications, and actual performance may vary over time. All operating parameters, including "typicals," must be validated for each customer application by customer's technical experts. NXP does not convey any license under its patent rights nor the rights of others. NXP sells products pursuant to standard terms and conditions of sale, which can be found at the following address: nxp.com/SalesTermsandConditions.

Right to make changes - NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Security — Customer understands that all NXP products may be subject to unidentified or documented vulnerabilities. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately. Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP. NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 19 May 2021
Document identifier: AN13198

arm