ARM® Cortex®-A57 MPCore Processor Cryptography Extension

Revision: r1p3

Technical Reference Manual

ARM DDI0514G

ARM® Cortex®-A57 MPCore Processor Cryptography Extension

Technical Reference Manual

Release Information

Document History

Issue	Date	Confidentiality	Change
A	04 June 2013	Non-Confidential	First release for r0p0
B	24 September 2013	Confidential	First release for r0p1
C	09 December 2013	Confidential	First release for r1p0
D	27 January 2014	Confidential	First release for r1p1
E	30 April 2014	Confidential	First release for r1p2
F	03 August 2014	Confidential	First release for r1p3
G	17 December 2015	Non-Confidential	Second release for r1p3

Non-Confidential Proprietary Notice

ARM Limited. Company 02557590 registered in England.

110 Fulbourn Road, Cambridge, England CB1 9NJ.

LES-PRE-20349

Confidentiality Status

This document is Non-Confidential. The right to use, copy and disclose this document may be subject to license restrictions in accordance with the terms of the agreement entered into by ARM and the party that ARM delivered this document to.

Unrestricted Access is an ARM internal classification.

Product Status

The information in this document is Final, that is for a developed product.

Web Address

http://www.arm.com

Contents

ARM® Cortex®-A57 MPCore Processor Cryptography Extension Technical Reference Manual

Preface

This preface introduces the *ARM® Cortex®-A57 MPCore Processor Cryptography Extension Technical Reference Manual*.

It contains the following:

Chapter 1
Introduction

This chapter introduces the Cryptography Extensions instructions for the Cortex-A57 processor and its features.

It contains the following sections:

1.1 About the Cortex-A57 processor Cryptography engine

The Cortex-A57 processor Cryptography engine supports the ARMv8 Cryptography Extensions. The Cryptography Extensions add new instructions that the Advanced SIMD can use to accelerate the execution of AES, SHA1, and SHA2-256 algorithms.

The following table lists the instructions for AES. See the *ARM® Architecture Reference Manual, ARMv8, for ARMv8-A architecture profile* for more information.

Table 1-1 AES instructions

Mnemonic	Instruction
AESD	AES single round decryption
AESE	AES single round encryption
AESIMC	AES inverse mix columns
AESMC	AES mix columns
VMULL[a]	Polynomial multiply long

The following table lists the instructions for SHA1 or SHA2-256. See the *ARM Architecture Reference Manual, ARMv8, for ARMv8-A architecture profile* for more information.

Table 1-2 SHA1 and SHA2-256 instructions

Mnemonic	Instruction
SHA1C	SHA1 hash update accelerator, choose
SHA1H	SHA1 fixed rotate
SHA1M	SHA1 hash update accelerator, majority
SHA1P	SHA1 hash update accelerator, parity
SHA1SU0	SHA1 schedule update accelerator, first part
SHA1SU1	SHA1 schedule update accelerator, second part
SHA256H	SHA256 hash update accelerator
SHA256H2	SHA256 hash update accelerator, upper part
SHA256SU0	SHA256 schedule update accelerator, first part
SHA256SU1	SHA256 schedule update accelerator, second part

[a] Polynomial 64-bit instruction.

1.2 Product revisions

This section describes the differences in functionality between product revisions.

r0p0 First release.

r0p1 No technical changes for cryptography extension.

r0p2 No technical changes for cryptography extension.

Chapter 2
Programmers Model

This chapter describes the registers of the Cryptography engine and provides information for programming the engine.

It contains the following sections:

2.1 About the programmers model

The Cortex-A57 processor Cryptography engine implements the Cryptography Extensions described in the ARMv8 architecture.

This section contains the following subsections:

2.1.1 Identifying the cryptography instructions implemented

Software can read a register to identify the cryptography instructions that are implemented.

The register to read depends on the Execution state, as follows:

AArch32

To access the ID_ISAR5 in AArch32 state, read the register with:

```
MRC p15, 0, <Rt>, c0, c2, 5 ; Read AArch32 Instruction Set Attribute Register 5
```

AArch64

To access the ID_ISAR5_EL1 in AArch64 state, read the register with:

```
MRS <Rd>, ID_ISAR5_EL1 ; Read AArch32 Instruction Set Attribute Register 5
```

To access the ID_AA64ISAR0_EL1 in AArch64 state, read the register with:

```
MRS <Xt>, ID_AA64ISAR0_EL1 ; Read AArch64 Instruction Set Attribute Register 0
```

The following table lists the instruction identification registers for the Cryptography engine. See the *ARM® Cortex®-A57 MPCore Processor Technical Reference Manual* for more information about the registers.

Table 2-1 Cryptography engine register summary

Name	Execution state	Description
ID_ISAR5	AArch32	AArch32 Instruction Set Attribute Register 5
ID_ISAR5_EL1	AArch64	
ID_AA64ISAR0_EL1		AArch64 Instruction Set Attribute Register 0

2.1.2 Disabling the Cryptography engine

The **CRYPTODISABLE[N:0]** input controls whether the Cryptography engine is disabled for processor `N`. The processor only samples this signal during reset.

When **CRYPTODISABLE** is HIGH, executing a cryptography instruction results in an Undefined Instruction exception.

Appendix A
Revisions

This appendix describes the technical changes between released issues of this book.

It contains the following sections:

- *A.1 Revisions* on page Appx-A-12.

A.1 Revisions

This appendix describes the technical changes between released issues of this book.

Table A-1 Issue A

Change	Location	Affects
First release	-	-

Table A-2 Differences between issue A and issue B

Change	Location	Affects
No technical changes	-	-

Table A-3 Differences between issue B and issue C

Change	Location	Affects
No technical changes	-	-

Table A-4 Differences between issue C and issue D

Change	Location	Affects
No technical changes	-	-

Table A-5 Differences between issue D and issue E

Change	Location	Affects
No technical changes	-	-

Table A-6 Differences between issue E and issue F

Change	Location	Affects
No technical changes	-	-

Table A-7 Differences between issue F and issue G

Change	Location	Affects
No technical changes	-	-