

# Arm® Cortex®-A75 Core Cryptographic Extension

Revision: r3p1

## Technical Reference Manual



# Arm® Cortex®-A75 Core Cryptographic Extension

## Technical Reference Manual

Copyright © 2016–2018 Arm Limited or its affiliates. All rights reserved.

### Release Information

### Document History

Issue	Date	Confidentiality	Change
0000-00	30 September 2016	Confidential	First release for r0p0
0100-00	12 December 2016	Confidential	First release for r1p0
0200-00	03 June 2017	Non-Confidential	First release for r2p0
0201-00	20 October 2017	Non-Confidential	First release for r2p1
0300-00	02 March 2018	Non-Confidential	First release for r3p0
0301-00	31 July 2018	Non-Confidential	First release for r3p1

### Non-Confidential Proprietary Notice

This document is protected by copyright and other related rights and the practice or implementation of the information contained in this document may be protected by one or more patents or pending patent applications. No part of this document may be reproduced in any form by any means without the express prior written permission of Arm. **No license, express or implied, by estoppel or otherwise to any intellectual property rights is granted by this document unless specifically stated.**

Your access to the information in this document is conditional upon your acceptance that you will not use or permit others to use the information for the purposes of determining whether implementations infringe any third party patents.

THIS DOCUMENT IS PROVIDED “AS IS”. ARM PROVIDES NO REPRESENTATIONS AND NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE DOCUMENT. For the avoidance of doubt, Arm makes no representation with respect to, and has undertaken no analysis to identify or understand the scope and content of, third party patents, copyrights, trade secrets, or other rights.

This document may include technical inaccuracies or typographical errors.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL ARM BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF ANY USE OF THIS DOCUMENT, EVEN IF ARM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

This document consists solely of commercial items. You shall be responsible for ensuring that any use, duplication or disclosure of this document complies fully with any relevant export laws and regulations to assure that this document or any portion thereof is not exported, directly or indirectly, in violation of such export laws. Use of the word “partner” in reference to Arm’s customers is not intended to create or refer to any partnership relationship with any other company. Arm may make changes to this document at any time and without notice.

If any of the provisions contained in these terms conflict with any of the provisions of any click through or signed written agreement covering this document with Arm, then the click through or signed written agreement prevails over and supersedes the conflicting provisions of these terms. This document may be translated into other languages for convenience, and you agree that if there is any conflict between the English version of this document and any translation, the terms of the English version of the Agreement shall prevail.

The Arm corporate logo and words marked with ® or ™ are registered trademarks or trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere. All rights reserved. Other brands and names mentioned in this document may be the trademarks of their respective owners. Please follow Arm’s trademark usage guidelines at <http://www.arm.com/company/policies/trademarks>.

Copyright © 2016–2018 Arm Limited (or its affiliates). All rights reserved.

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®-A75 Core Cryptographic Extension Technical Reference Manual

### **Preface**

<i>About this book</i> .....	6
<i>Feedback</i> .....	8

### **Chapter 1**

#### **Functional description**

1.1	<i>About the Cryptographic Extension</i> .....	1-10
1.2	<i>Revisions</i> .....	1-11

### **Chapter 2**

#### **Register descriptions**

2.1	<i>Identifying the cryptographic instructions implemented</i> .....	2-13
2.2	<i>Disabling the Cryptographic Extension</i> .....	2-14
2.3	<i>Register summary</i> .....	2-15
2.4	<i>ID_AA64ISAR0_EL1, AArch64 Instruction Set Attribute Register 0, EL1</i> .....	2-16
2.5	<i>ID_ISAR5_EL1, AArch32 Instruction Set Attribute Register 5, EL1</i> .....	2-18
2.6	<i>ID_ISAR5, Instruction Set Attribute Register 5</i> .....	2-20

### **Appendix A**

#### **Revisions**

A.1	<i>Revisions</i> .....	Appx-A-23
-----	------------------------	-----------

# Preface

This preface introduces the *Arm® Cortex®-A75 Core Cryptographic Extension Technical Reference Manual*.

It contains the following:

- [About this book](#) on page 6.
- [Feedback](#) on page 8.

## About this book

This document describes the optional cryptographic features of the Cortex®-A75 core. It includes descriptions of the registers used by the Cryptographic Extension.

### Product revision status

The *rm**pn* identifier indicates the revision status of the product described in this book, for example, r1p2, where:

*rm* Identifies the major revision of the product, for example, r1.

*pn* Identifies the minor revision or modification status of the product, for example, p2.

### Intended audience

This manual is for system designers, system integrators, and programmers who are designing or programming a System-on-Chip (SoC) that uses the Cortex®-A75 core with the optional Cryptographic Extension.

### Using this book

This book is organized into the following chapters:

#### **Chapter 1 Functional description**

This chapter describes the Cortex-A75 core Cryptographic Extension.

#### **Chapter 2 Register descriptions**

This chapter describes the Cryptographic Extension registers.

#### **Appendix A Revisions**

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

### Glossary

The Arm® Glossary is a list of terms used in Arm documentation, together with definitions for those terms. The Arm Glossary does not contain terms that are industry standard unless the Arm meaning differs from the generally accepted meaning.

See the [Arm® Glossary](#) for more information.

### Typographic conventions

#### *italic*

Introduces special terminology, denotes cross-references, and citations.

#### **bold**

Highlights interface elements, such as menu names. Denotes signal names. Also used for terms in descriptive lists, where appropriate.

#### `monospace`

Denotes text that you can enter at the keyboard, such as commands, file and program names, and source code.

#### monospace

Denotes a permitted abbreviation for a command or option. You can enter the underlined text instead of the full command or option name.

#### `monospace italic`

Denotes arguments to monospace text where the argument is to be replaced by a specific value.

#### `monospace bold`

Denotes language keywords when used outside example code.

<and>

Encloses replaceable terms for assembler syntax where they appear in code or code fragments.  
For example:

```
MRC p15, 0, <Rd>, <CRn>, <CRm>, <Opcode_2>
```

SMALL CAPITALS

Used in body text for a few terms that have specific technical meanings, that are defined in the *Arm® Glossary*. For example, IMPLEMENTATION DEFINED, IMPLEMENTATION SPECIFIC, UNKNOWN, and UNPREDICTABLE.

## Additional reading

This book contains information that is specific to this product. See the following documents for other relevant information:

### Arm publications

- *Arm® Cortex®-A75 Core Technical Reference Manual* (100403).
- *Arm® Cortex®-A75 Core Integration Manual* (100405).
- *Arm® Cortex®-A75 Core Configuration and Sign-off Guide* (100404).
- *Arm® Architecture Reference Manual Armv8, for Armv8-A architecture profile* (DDI 0487).

### Other publications

- *Advanced Encryption Standard*. (FIPS 197, November 2001).
- *Secure Hash Standard (SHS)* (FIPS 180-4, March 2012).

## Feedback

### Feedback on this product

If you have any comments or suggestions about this product, contact your supplier and give:

- The product name.
- The product revision or version.
- An explanation with as much information as you can provide. Include symptoms and diagnostic procedures if appropriate.

### Feedback on content

If you have comments on content then send an e-mail to [errata@arm.com](mailto:errata@arm.com). Give:

- The title *Arm Cortex-A75 Core Cryptographic Extension Technical Reference Manual*.
- The number 100458\_0301\_00\_en.
- If applicable, the page number(s) to which your comments refer.
- A concise explanation of your comments.

Arm also welcomes general suggestions for additions and improvements.

————— **Note** —————

Arm tests the PDF only in Adobe Acrobat and Acrobat Reader, and cannot guarantee the quality of the represented document when used with any other PDF reader.

---



# Chapter 1

## Functional description

This chapter describes the Cortex-A75 core Cryptographic Extension.

It contains the following sections:

- [1.1 About the Cryptographic Extension on page 1-10.](#)
- [1.2 Revisions on page 1-11.](#)

## 1.1 About the Cryptographic Extension

The Cortex-A75 core Cryptographic Extension supports the Armv8-A Cryptographic Extension.

The Cryptographic Extension adds new A64, A32, and T32 instructions to Advanced SIMD that accelerate *Advanced Encryption Standard* (AES) encryption and decryption. It also adds instructions to implement the *Secure Hash Algorithm* (SHA) functions SHA-1, SHA-224, and SHA-256.

---

**Note**

The optional Cryptographic Extension is not included in the base product. Arm supplies the Cryptographic Extension only under an additional license to the Cortex-A75 core and Advanced SIMD and floating-point support licenses.

---

## 1.2 Revisions

This section describes the differences in functionality between product revisions.

- r0p0** First release.
- r1p0** Second release. There are no technical changes.
- r2p0** Third release. There are no technical changes.
- r2p1** Fourth release. There are no technical changes.
- r3p0** Fifth release. There are no technical changes.
- r3p1** Sixth release. There are no technical changes.

# Chapter 2

## Register descriptions

This chapter describes the Cryptographic Extension registers.

It contains the following sections:

- [2.1 Identifying the cryptographic instructions implemented](#) on page 2-13.
- [2.2 Disabling the Cryptographic Extension](#) on page 2-14.
- [2.3 Register summary](#) on page 2-15.
- [2.4 ID\\_AA64ISAR0\\_EL1, AArch64 Instruction Set Attribute Register 0, EL1](#) on page 2-16.
- [2.5 ID\\_ISAR5\\_EL1, AArch32 Instruction Set Attribute Register 5, EL1](#) on page 2-18.
- [2.6 ID\\_ISAR5, Instruction Set Attribute Register 5](#) on page 2-20.

## 2.1 Identifying the cryptographic instructions implemented

Software can identify the cryptographic instructions that are implemented by reading three registers.

The three registers are:

- ID\_AA64ISAR0\_EL1 in the AArch64 execution state.
- ID\_ISAR5\_EL1 in the AArch64 execution state.
- ID\_ISAR5 in the AArch32 execution state.

## 2.2 Disabling the Cryptographic Extension

To disable the Cryptographic Extension, assert the **CRYPTODISABLE** input signal that applies to all the Cortex-A75 cores present in a cluster. This signal is sampled only during reset of the cores.

When **CRYPTODISABLE** is asserted:

- Executing a cryptographic instruction results in an **UNDEFINED** exception.
- The ID registers described in *Table 2-1 Cryptographic Extension register summary on page 2-15* indicate that the Cryptographic Extension is not implemented.

## 2.3 Register summary

The Cortex-A75 core has three instruction identification registers. Each register has a specific purpose, usage constraints, configurations, and attributes.

The following table lists the instruction identification registers for the Cortex-A75 core Cryptographic Extension.

**Table 2-1 Cryptographic Extension register summary**

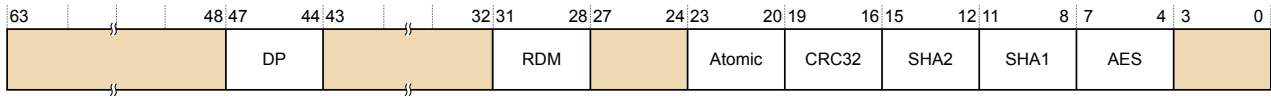
Name	Execution state	Description
ID_AA64ISAR0_EL1	AArch64	See <a href="#">2.4 ID_AA64ISAR0_EL1</a> , <i>AArch64 Instruction Set Attribute Register 0, EL1</i> on page 2-16.
ID_ISAR5_EL1	AArch64	See <a href="#">2.5 ID_ISAR5_EL1</a> , <i>AArch32 Instruction Set Attribute Register 5, EL1</i> on page 2-18.
ID_ISAR5	AArch32	See <a href="#">2.6 ID_ISAR5</a> , <i>Instruction Set Attribute Register 5</i> on page 2-20.

## 2.4 ID\_AA64ISAR0\_EL1, AArch64 Instruction Set Attribute Register 0, EL1

The ID\_AA64ISAR0\_EL1 provides information about the instructions implemented in AArch64 state, including the instructions provided by the Cryptographic Extension.

### Bit field descriptions

ID\_AA64ISAR0\_EL1 is a 64-bit register.



RES0

Figure 2-1 ID\_AA64ISAR0\_EL1 bit assignments

### RES0, [63:48]

RES0 Reserved.

### DP, [47:44]

Indicates whether Dot Product support instructions are implemented.

0x1 UDOT, SDOT instructions are implemented.

### RES0, [43:32]

RES0 Reserved.

### RDM, [31:28]

Indicates whether *Rounding Double Multiply* (RDM) instructions are implemented. The value is:

0x1 SQRDMLAH and SQRDMLSH instructions are implemented.

### [27:24]

RES0 Reserved.

### Atomic, [23:20]

Indicates whether atomic instructions are implemented. The value is:

0x2 LDADD, LDCLR, LDEOR, LDSET, LDSMAX, LDSMIN, LDUMAX, LDUMIN, CAS, CASP, and SWP instructions are implemented.

### CRC32, [19:16]

Indicates whether CRC32 instructions are implemented. The value is:

0x1 CRC32 instructions are implemented.

### SHA2, [15:12]

Indicates whether SHA2 instructions are implemented. The possible values are:

0x0 No SHA2 instructions are implemented. This is the value if the core implementation does not include the Cryptographic Extension.

0x1 SHA256H, SHA256H2, SHA256U0, and SHA256U1 are implemented. This is the value if the core implementation includes the Cryptographic Extension.

### SHA1, [11:8]



Indicates whether SHA1 instructions are implemented. The possible values are:

- 0x0 No SHA1 instructions are implemented. This is the value if the core implementation does not include the Cryptographic Extension.
- 0x1 SHA1C, SHA1P, SHA1M, SHA1SU0, and SHA1SU1 are implemented. This is the value if the core implementation includes the Cryptographic Extension.

#### AES, [7:4]

Indicates whether AES instructions are implemented. The possible values are:

- 0x0 No AES instructions implemented. This is the value if the core implementation does not include the Cryptographic Extension.
- 0x2 AESE, AESD, AESMC, and AESIMC are implemented, plus PMULL and PMULL2 instructions operating on 64-bit data. This is the value if the core implementation includes the Cryptographic Extension.

#### [3:0]

RES0 Reserved.

#### Configurations

ID\_AA64ISAR0\_EL1 is architecturally mapped to external register ID\_AA64ISAR0.

#### Usage constraints

##### Accessing the ID\_AA64ISAR0\_EL1

To access the ID\_AA64ISAR0\_EL1:

```
MRS <Xt>, ID_AA64ISAR0_EL1 ; Read ID_AA64ISAR0_EL1 into Xt
```

Register access is encoded as follows:

**Table 2-2 ID\_AA64ISAR0\_EL1 access encoding**

op0	op1	CRn	CRm	op2
11	000	0000	0110	000

#### Accessibility

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	RO	RO	RO	RO	RO

## 2.5 ID\_ISAR5\_EL1, AArch32 Instruction Set Attribute Register 5, EL1

The AArch64 register ID\_ISAR5\_EL1 provides information about the instructions implemented in AArch32 state, including the instructions provided by the optional Cryptographic Extension.

### Bit field descriptions

ID\_ISAR5\_EL1 is a 32-bit register.

31	28	27	24	23	20	19	16	15	12	11	8	7	4	3	0		
				RDM				CRC32		SHA2		SHA1		AES		SEVL	

 RES0

Figure 2-2 ID\_ISAR5\_EL1 bit assignments

#### [31:28]

 Reserved.

#### RDM, [27:24]

Indicates whether RDM instructions are implemented. The value is:

0x1 SQRDMLAH and SQRDMLSH instructions are implemented.

#### [23:20]

 Reserved.

#### CRC32, [19:16]

Indicates whether CRC32 instructions are implemented in AArch32 state. The value is:

0x1 CRC32 instructions are implemented.

#### SHA2, [15:12]

Indicates whether SHA2 instructions are implemented in AArch32 state. The possible values are:

0x0 Cryptographic Extension is not implemented or is disabled.

0x1 SHA256H, SHA256H2, SHA256SU0, and SHA256SU1 instructions are implemented.

#### SHA1, [11:8]

Indicates whether SHA1 instructions are implemented in AArch32 state. The possible values are:

0x0 Cryptographic Extension is not implemented or is disabled.

0x1 SHA1C, SHA1P, SHA1M, SHA1H, SHA1SU0, and SHA1SU1 instructions are implemented.

#### AES, [7:4]

Indicates whether AES instructions are implemented in AArch32 state. The possible values are:

0x0 Cryptographic Extension is not implemented or is disabled.

0x2 AESE, AESD, AESMC, and AESIMC are implemented, plus PMULL and PMULL2 instructions operating on 64-bit data.

**SEVL, [3:0]**

Indicates whether the SEVL instruction is implemented. The value is:

0x1      SEVL implemented to send event local.

**Configurations**

ID\_ISAR5\_EL1 is architecturally mapped to AArch32 register ID\_ISAR5. See [2.6 ID\\_ISAR5, Instruction Set Attribute Register 5](#) on page 2-20.

**Usage constraints**

**Accessing the ID\_ISAR5\_EL1**

To access the ID\_ISAR5\_EL1:

```
MRS <Xt>, ID_ISAR5_EL1 ; Read ID_ISAR5_EL1 into Xt
```

Register access is encoded as follows:

**Table 2-3 ID\_ISAR5\_EL1 access encoding**

op0	op1	CRn	CRm	op2
11	000	0000	0010	101

**Accessibility**

This register is accessible as follows:

EL0	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	RO	RO	RO	RO	RO

## 2.6 ID\_ISAR5, Instruction Set Attribute Register 5

The AArch32 register ID\_ISAR5 provides information about the instructions implemented in AArch32 state, including the instructions provided by the optional Cryptographic Extension.

### Bit field descriptions

ID\_ISAR5 is a 32-bit register.

31	28	27	24	23	20	19	16	15	12	11	8	7	4	3	0		
				RDM				CRC32		SHA2		SHA1		AES		SEVL	

RES0

Figure 2-3 ID\_ISAR5 bit assignments

#### [31:28]

RES0 Reserved.

#### RDM, [27:24]

Indicates whether RDM instructions are implemented. The value is:

0x1 SQRDMLAH and SQRDMLSH instructions are implemented.

#### [23:20]

RES0 Reserved.

#### CRC32, [19:16]

Indicates whether CRC32 instructions are implemented in AArch32 state. The value is:

0x1 CRC32 instructions are implemented.

#### SHA2, [15:12]

Indicates whether SHA2 instructions are implemented in AArch32 state. The possible values are:

0x0 Cryptographic extension is not implemented or is disabled.

0x1 SHA256H, SHA256H2, SHA256SU0, and SHA256SU1 instructions are implemented.

#### SHA1, [11:8]

Indicates whether SHA1 instructions are implemented in AArch32 state. The possible values are:

0x0 Cryptographic Extension is not implemented or is disabled.

0x1 SHA1C, SHA1P, SHA1M, SHA1H, SHA1SU0, and SHA1SU1 instructions are implemented.

#### AES, [7:4]

Indicates whether AES instructions are implemented in AArch32 state. The possible values are:

0x0 Cryptographic Extension is not implemented or is disabled.

0x2 AESE, AESD, AESMC and AESIMC, plus PMULL and PMULL2 instructions operating on 64-bit data.

## SEVL, [3:0]

Indicates whether the SEVL instruction is implemented. The value is:

0x1 SEVL implemented to send event local.

## Configurations

ID\_ISAR5 is architecturally mapped to AArch64 register ID\_ISAR5\_EL1. See [2.5 ID\\_ISAR5\\_EL1, AArch32 Instruction Set Attribute Register 5, EL1](#) on page 2-18.

There is one copy of this register that is used in both Secure and Non-secure states.

## Usage constraints

### Accessing the ID\_ISAR5

To access ID\_ISAR5:

```
MRC p15, 0, <Rt>, c0, c2, 5; Read ID_ISAR5 into Rt
```

This register is accessible as follows:

EL0 (NS)	EL0 (S)	EL1 (NS)	EL1 (S)	EL2	EL3 (SCR.NS = 1)	EL3 (SCR.NS = 0)
-	-	RO	RO	RO	RO	RO

# Appendix A

## Revisions

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

It contains the following section:

- [A.1 Revisions on page Appx-A-23](#).

## A.1 Revisions

This section describes the technical changes between released issues of this document.

**Table A-1 Issue 0000-00**

Change	Location	Affects
First release for r0p0	-	-

**Table A-2 Differences between Issue 0000-00 and Issue 0100-00**

Change	Location	Affects
First release for r1p0	Document history table.	r1p0
ID_AA64ISAR0_EL1 bit diagram updated	<a href="#">2.4 ID_AA64ISAR0_EL1, AArch64 Instruction Set Attribute Register 0, EL1 on page 2-16.</a>	r1p0

**Table A-3 Differences between Issue 0100-00 and Issue 0200-00**

Change	Location	Affects
First release for r2p0	Document history table.	r2p0

**Table A-4 Differences between Issue 0200-00 and Issue 0201-00**

Change	Location	Affects
First release for r2p1	Document history table	r2p1
ARM updated to Arm to reflect company rebranding	Entire manual	r2p1

**Table A-5 Differences between Issue 0201-00 and Issue 0300-00**

Change	Location	Affects
First release for r3p0	Document history table	r3p0

**Table A-6 Differences between Issue 0300-00 and Issue 0301-00**

Change	Location	Affects
First release for r3p1	Document history table	r3p1