ARM® Cortex®-A32 Processor Cryptographic Extension

Revision: r0p1

Technical Reference Manual

ARM

ARM 100242_0001_00_en

ARM® Cortex®-A32 Processor Cryptographic Extension

Technical Reference Manual

Release Information

Document History

Issue	Date	Confidentiality	Change
0000-00	18 March 2016	Confidential	First release for r0p0
0001-00	04 March 2017	Non-Confidential	First release for r0p1

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®-A32 Processor Cryptographic Extension Technical Reference Manual

Preface

This preface introduces the *ARM® Cortex®-A32 Processor Cryptographic Extension Technical Reference Manual*.

It contains the following:

About this book

A technical reference document that describes the optional cryptographic features of the Cortex®-A32 processor. It includes descriptions of the registers used by the Cryptographic Extension.

Product revision status

The r*m*p*n* identifier indicates the revision status of the product described in this book, for example, r*1*p*2*, where:

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

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

Intended audience

This manual is written for system designers, system integrators, and programmers who are designing or programming a System-on-Chip (SoC) that uses the Cortex®-A32 processor with the optional Cryptographic Extension.

Using this book

This book is organized into the following chapters:

Chapter 1 Functional Description
This chapter describes the Cryptographic Extension for the Cortex-A32 processor.

Chapter 2 Register Descriptions
This chapter describes the AArch32 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.

`mono`space
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.

Timing diagrams

The following figure explains the components used in timing diagrams. Variations, when they occur, have clear labels. You must not assume any timing information that is not explicit in the diagrams.

Shaded bus and signal areas are undefined, so the bus or signal can assume any value within the shaded area at that time. The actual level is unimportant and does not affect normal operation.

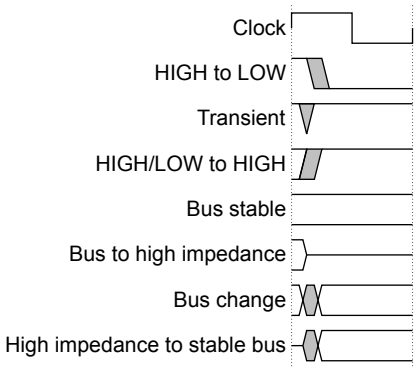

Figure 1 Key to timing diagram conventions

Signals

The signal conventions are:

Signal level
: The level of an asserted signal depends on whether the signal is active-HIGH or active-LOW. Asserted means:
- HIGH for active-HIGH signals.
- LOW for active-LOW signals.

Lowercase n
: At the start or end of a signal name denotes an active-LOW signal.

Additional reading

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

ARM publications
- *ARM® Cortex®-A32 Processor Technical Reference Manual* (ARM 100241).
- *ARM® Cortex®-A32 Configuration and Sign-off Guide* (ARM 100244).
- *ARM® Cortex®-A32 Processor Integration Manual* (ARM 100245).
- *ARM® Cortex®-A32 Processor Advanced SIMD and Floating-point Support Technical Reference Manual* (ARM 100243).
- *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* (ARM 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*. Give:

- The title *ARM® Cortex®-A32 Processor Cryptographic Extension Technical Reference Manual*.
- The number ARM 100242_0001_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 Cryptographic Extension for the Cortex-A32 processor.

It contains the following sections:

1.1 About the Cryptographic Extension

The Cortex-A32 processor Cryptographic Extension supports the ARMv8 Cryptographic Extensions.

The Cryptographic Extension adds new A32 and T32 instructions to Advanced SIMD that accelerate *Advanced Encryption Standard* (AES) encryption and decryption. It also adds 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-A32 processor and Advanced SIMD and floating-point support licenses.

1.2 Revisions

This section describes the differences in functionality between product revisions.

r0p0 First release.

r0p1 There are no functional changes in this revision.

Chapter 2
Register Descriptions

This chapter describes the AArch32 Cryptographic Extension registers.

It contains the following sections:

2.1 Identifying the cryptographic instructions implemented

Software can identify the cryptographic instructions implemented by reading one register.

This register is ID_ISAR5. See also *2.3 Instruction Set Attribute Register 5* on page 2-16.

2.2 Disabling the Cryptographic Extension

To disable the Cryptographic Extension for each individual core, assert the corresponding bit of the **CRYPTODISABLE** input signal. This signal is only sampled during reset of the core.

When **CRYPTODISABLE** is asserted:

- Executing a cryptographic instruction results in an UNDEFINED exception.
- The ID register described in *2.3 Instruction Set Attribute Register 5* on page 2-16 indicates that the Cryptographic Extension is not implemented.

2.3 Instruction Set Attribute Register 5

The ID_ISAR5 characteristics are:

Purpose

Provides information about the instructions implemented in AArch32 state, including the instructions provided by the optional Cryptographic Extension.

Note

The optional Cryptographic Extension is not included in the base product of the processor. ARM requires licensees to have contractual rights to obtain the Cryptographic Extension.

Usage constraints

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

The ID_ISAR5 must be interpreted with ID_ISAR0, ID_ISAR1, ID_ISAR2, ID_ISAR3, and ID_ISAR4.

Configurations

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

Attributes

ID_ISAR5 is a 32-bit register.

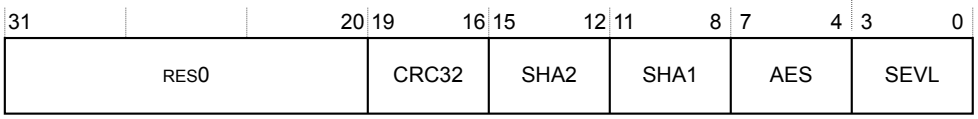

Figure 2-1 ID_ISAR5 bit assignments

[31:20]

Reserved, RES0.

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 extensions are not implemented or are 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 extensions are not implemented or are 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 extensions are not implemented or are 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.

To access ID_ISAR5:

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

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-19.

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 Issue 0001-00

Change	Location	Affects
First release for r0p1	On front page and in document history table.	r0p1