Arm® TrustZone® TRNG

Revision: r0p0

Characterization Application Note

100685_0000_06_en

Arm® TrustZone® TRNG

Characterization Application Note

Release Information

Document History

Issue	Date	Confidentiality	Change
00	27 July 2015	Confidential	First official release (v1.0).
01	08 October 2015	Confidential	Second release (v1.1).
02	22 November 2015	Confidential	Third release (v1.2).
03	27 January 2016	Confidential	Fourth release (v1.3).
04	17 May 2016	Confidential	Fifth release (v1.4).
05	08 November 2016	Confidential	Sixth release.
06	09 January 2018	Non-Confidential	Seventh release.

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*.

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® TrustZone® TRNG Characterization Application Note

Preface

About this book 6

Chapter 1 **Overview of Arm® TrustZone® TRNG**

1.1 TRNG characterization 1-9

Chapter 2 **TRNG characterization procedure**

2.1 Characterization procedure overview 2-11

2.2 Characterization test program 2-12

2.3 Characterization test conditions 2-13

2.4 Base iteration 2-14

2.5 First characterization iteration 2-15

2.6 Second characterization iteration 2-16

Appendix A **CC_TST_TRNG output**

A.1 CC_TST_TRNG output format Appx-A-18

Appendix B **Revisions**

B.1 Revision history Appx-B-20

Preface

This preface introduces the *Arm® TrustZone® TRNG Characterization Application Note*.

It contains the following:

- *About this book* on page 6.

About this book

This book describes the characterization process for the Arm TrustZone® True Random Number Generator (TRNG).

Using this book

This book is organized into the following chapters:

Chapter 1 Overview of Arm® TrustZone® TRNG
This chapter provides an overview of the Arm TrustZone® TRNG and its characterization.

Chapter 2 TRNG characterization procedure
This chapter provides the detailed Arm characterization procedure.

Appendix A CC_TST_TRNG output
This appendix describes the format of `CC_TST_TRNG` output.

Appendix B 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.

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 TrustZone TRNG Characterization Application Note*.
- The number 100685_0000_06_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.

Other information

- *Arm® Developer*.
- *Arm® Information Center*.
- *Arm® Technical Support Knowledge Articles*.
- *Technical Support*.
- *Arm® Glossary*.

Chapter 1
Overview of Arm® TrustZone® TRNG

This chapter provides an overview of the Arm TrustZone® TRNG and its characterization.

It contains the following section:

- *1.1 TRNG characterization* on page 1-9.

1.1 TRNG characterization

Arm TrustZone True Random Number Generator (TRNG) configuration parameters specify the settings of the internal ring-oscillator lengths, and the output sampling rate. The parameters are device-specific.

Each silicon process has different noise and jitter characteristics. The specific SoC layout affects these characteristics. Therefore, the TRNG behavior must be characterized on the actual silicon of the device to determine the most suitable parameters. Characterizing in this way ensures that the TRNG output has maximal entropy.

Characterization must be performed during the initial post-silicon testing of the device, or whenever substantial changes are made. For example, after changes to process or respins.

Chapter 2
TRNG characterization procedure

This chapter provides the detailed Arm characterization procedure.

It contains the following sections:

- *2.1 Characterization procedure overview* on page 2-11.
- *2.2 Characterization test program* on page 2-12.
- *2.3 Characterization test conditions* on page 2-13.
- *2.4 Base iteration* on page 2-14.
- *2.5 First characterization iteration* on page 2-15.
- *2.6 Second characterization iteration* on page 2-16.

2.1 Characterization procedure overview

The characterization procedure requires two iterations between the partner and Arm.

In each iteration, the partner performs a series of characterization tests, and sends the resulting data to Arm. Arm analyzes the results, and returns the best Arm settings to the partner.

Following is a high-level overview of the characterization procedure:

Table 2-1 Characterization high-level procedure steps

Step	Owner	Execution	Comments
Prepare characterization test program.	Partner	Prepare a characterization test program that uses the `CC_TST_TRNG` routine that Arm supplies.	See *2.2 Characterization test program* on page 2-12 and *2.3 Characterization test conditions* on page 2-13.
Base iteration: Find the minimal sample count.	Partner	Run the preliminary test to establish the minimal (base) value of the sample count.	See *2.4 Base iteration* on page 2-14.
First iteration: Run first set of characterization tests.	Partner	Run a series of characterization tests under multiple test conditions.	See *2.5 First characterization iteration* on page 2-15. Send results to Arm.
First iteration: Analyze first characterization test results.	Arm	Runs a set of statistical tests on the characterization output data.	Send the partner the TRNG configuration parameters, and a set of corners to run the tests on.
Second iteration: Run second set of characterization tests.	Partner	1. Use `CC_TST_TRNG` with the configuration parameters that were received in the first iteration. 2. Run the characterization tests in typical and worst-case conditions, as provided by Arm.	See *2.6 Second characterization iteration* on page 2-16. Send results to Arm.
Second iteration: Analyze second characterization test results.	Arm	Runs a set of statistical tests on the characterization output data. Use this analysis to generate the mass production Arm TrustZone TRNG configuration parameters.	Send the mass production parameters to the partner. **Note** If the results are not good enough, you might have to repeat the second iteration.

2.2 Characterization test program

The partner must implement the characterization test program, using the `CC_TST_TRNG` API that Arm supplies.

Example of API

```
/**
 * Collect TRNG output for characterization
 *
 * @regBaseAddress: Base address of the TRNG registers in the system memory map
 * @TRNGMode: 0 – 1st iteration; 1 – 2nd iteration, FE TRNG driver; 2 – 2nd iteration,
800-90B TRNG driver
 * @roscLength: Ring oscillator id (0 to 3)
 * @sampleCount: Ring oscillator sampling rate
 * @buffSize: Size of buffer passed in dataBuff_ptr
 * @dataBuff_ptr: Buffer for results
 *
 * The function's output is 0 if the collection succeeds, or a (non-zero)
 * error code on failure.
 */
 int CC_TST_TRNG( unsigned int regBaseAddress,
                  unsigned int TRNGMode,
                  unsigned int roscLength,
                  unsigned int sampleCount,
                  unsigned int buffSize,
                  unsigned int *dataBuff_ptr);
```

2.3 Characterization test conditions

Each characterization test is executed by running the characterization test program under a combination of conditions.

These tests are described in *Table 2-2 Characterization test conditions* on page 2-13.

It is critical that for each test:

- All output bits are collected using a single contiguous execution of the test.
- All the resulting bits are saved in the output file without any gaps.

If any bits are dropped and not captured in the output file, the test must be rerun as the statistical analysis of the output is meaningless.

Table 2-2 Characterization test conditions

Configuration variable	Operating conditions	Filename values
Ring oscillator length.	The four configurable lengths that Arm TrustZone TRNG allows.	R0, R1, R2, R3. R0 is the shortest length and R3 is the longest. **Note** In some chips, the ring oscillator might not properly work when configured to the shorter lengths.
Voltage.	High, typical, low.	VH, VT, VL.
Temperature.	High, typical, low.	TH, TT, TL.
CMOS process corner.	Typical, fast/fast, fast/slow, slow/fast, slow/slow.	CT, CFF, CFS, CSF, CSS.

This section contains the following subsection:

- *2.3.1 Output-file names* on page 2-13.

2.3.1 Output-file names

Output-files are named according to a standard format.

The output file for each characterization test is named according to the Filename Values column in *Table 2-2 Characterization test conditions* on page 2-13. Output filename format is `trng_samples_R*_S*_V*_T*_C*.bin`.

For example, for the following characterization test:

- The longest ring oscillator length.
- Sample counter value of five.
- High voltage.
- Low temperature.
- Fast or slow CMOS corner.

The filename is `trng_samples_R3_S5_VH_TL_CFS.bin`.

2.4 Base iteration

The base iteration is used to find the minimum sample counter value for which Arm TrustZone TRNG operates properly, under typical operating conditions.

These conditions are:

- The second-longest ring-oscillator.
- Typical voltage.
- Typical temperature.
- Typical process corner.

The minimum sample counter value is found by calling `CC_TST_TRNG` with increasing values of `sampleCount` (starting with 1) until it exits successfully.

Note

In many systems, the test succeeds immediately (with `sampleCount=1`), which is an expected and even desirable result.

Finding minimum sample counter value:

```
/* Buffer size should be at least 25K Bytes (200K bits) */
#define BUF_SIZE    (25*1000)
#define TRNG_TST_OK  0
    char Buffer[BUF_SIZE];
    int sampleCount;
    for (sampleCount = 1; ; sampleCount ++) {
        int rv = CC_TST_TRNG(
                    /* regBaseAddress = */  TRNG_HW_ADDRESS,
                    /* TRNGMode = */        0,
                    /* roscLength = */      2,
                    /* sampleCount = */     sampleCount,
                    /* buffSize = */        sizeof(Buffer),
                    /* dataBuff_ptr = */    Buffer);
        if (rv == TRNG_TST_OK) break;
    }
    minValidSampleCount = sampleCount;
```

2.5 First characterization iteration

Perform this procedure for each of the characterization test conditions combinations.

For more details, see *Table 2-2 Characterization test conditions* on page 2-13.

1. Set up the test operating conditions.
2. Run `CC_TST_TRNG` under these conditions with `sampleCount` values of:
   - First set: S_{SMP1} = The minimal `sampleCount` found in *2.4 Base iteration* on page 2-14.
   - Second set: S_{SMP2} = Ceiling(1.5 * (S_{SMP1}+1)-1).
   - Third set: S_{SMP3} = Ceiling(1.5 * (S_{SMP2}+1)-1).

   For example, if the minimum value of `sampleCount` is 8, then run `CC_TST_TRNG` under each of the 180 conditions with:
   - `SMP1=8` in the first set.
   - `SMP2=13` in the second set.
   - `SMP3=20` in the third set.
3. Save the results of each test run in the relevant output file that is named according to *2.3.1 Output-file names* on page 2-13.

Overall, the partner must run a total of 540 characterization tests: (3 (sample counter values) * 4 (ring oscillator configurations) * 3 (voltages) * 3 (temperatures) * 5 (process corners).

The estimated total time for the characterization procedure is between 16-18 hours: 5 chips * 3 temperature conditions * (30 minutes to set each chip in each temperature condition + [30-40] minutes for running all oscillator, voltage, and sample count combinations in this temperature).

The outcome of this iteration is:

- A set of four sample count values – one value for each ring oscillator length.
- A definition of the typical corner (voltage/temperature/process) to be used for the second characterization iteration.
- A definition of the worst-case corner (voltage/temperature/process) to be used for the second characterization iteration.

2.6 Second characterization iteration

You must run a second set of characterization tests to determine the TRNG configuration parameters.

For each of the corners that Arm identifies as result of the first iteration, run four characterization tests by calling `CC_TST_TRNG` with each of the four ring oscillator lengths (each with its corresponding sample count).

Depending on the intended TRNG driver, each call to `CC_TST_TRNG` must be as follows:

- FE TRNG driver: Call `CC_TST_TRNG` with `TRNGMode=1` and collect 100Mbit (12.5MB).
- 800-90B TRNG driver: `CC_TST_TRNG` with `TRNGMode=2` and collect 10Mbit (1.25MB).

The same output file naming rules apply for both drivers. For more information, see *2.3.1 Output-file names* on page 2-13.

Note

As with the first-iteration tests, it is critical that:

- All output bits are collected using a single contiguous execution of the test.
- All resulting bits are saved in the output file without any gaps.

If any bits are dropped and not captured in the output file. Then, rerun the test as the statistical analysis of the output is meaningless.

If the system does not have sufficient memory to collect all required bits in a single run, you can split each test into multiple runs. For example 100 consecutive runs, each collecting 1Mbits.

The partner must send the resulting output files to Arm for statistical analysis. The returned result is the final TRNG configuration that is used for mass production. These configuration values must be updated in the relevant header files of the TRNG driver.

Note

If there are errors, the partner must repeat this iteration, or parts of it (some of the ring oscillator lengths) until a full set is obtained.

Appendix A
CC_TST_TRNG output

This appendix describes the format of `CC_TST_TRNG` output.

It contains the following section:

- *A.1 CC_TST_TRNG output format* on page Appx-A-18.

A.1 CC_TST_TRNG output format

When CC_TST_TRNG is run, in addition to collecting samples, it stores some metadata in its output buffer. This buffer is described in terms of 32-bit little-endian words.

The following table lists the value of each word:

Table A-1 CC_TST_TRNG output format

Buffer offset (32-bit words)	Value
0	Signature value: 0xAABBCCDD.
1	• Bits [23:0] - buffSize. • Bits [25:24] - roscLength. • Bits [31:31] - TRNGMode.
2	sampleCount
3	Signature value: 0xAABBCCDD.
4..N-1	Collected samples. Each 32-bit word contains the first collected sample in bit 0, and the last collected sample in bit 31.
N	Signature value: 0xDDCCBBAA.
N+1	Error flags • Bit [0] - Samples were lost during collection. • Bit [1] - Autocorrelation error occurred. • Bit [2] - CRNGT error that is detected and recovered. • Bit [3] - Input that is stuck at same level for 32 bits.
N+2	Signature value: 0xDDCCBBAA.

Note

The value of "N" is derived from the buffer size, and is calculated to fit the entire data in the supplied buffer (as per the buffSize argument).

When parsing the output, it is important to test that the signature value is correct.

Appendix B
Revisions

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

It contains the following section:

- *B.1 Revision history* on page Appx-B-20.

B.1 Revision history

Table B-1 Issue 00 (v1.0)

Change	Location
First release.	-

Table B-2 Differences between issue 00 (v1.0) and issue 01 (v1.1)

Change	Location
Rebranded template to Arm logo and colors.	Entire document.
Product renamed Arm RNG.TrustZone.	Entire document.
`DX_TST_TRNG` renamed `CC_TST_TRNG`.	Entire document.
Added the following standards: • *BSI AIS-31: Functionality Classes and Evaluation Methodology for True Random Number Generators* • *NIST SP 90A: Recommendation for Random Number Generation Using Deterministic Random Bit Generators – App C.*	*Referenced Documents*
Added STRNG driver operating mode.	*ArmTrustZone RNG Overview*
Added STRNG driver to `TRNGMode` values in `CC_TST_TRNG` API code block.	*First Characterization Test Program.* on page 2-15
Added STRNG driver.	*Second Characterization Test Program* on page 2-16
Added STRNG driver to `TRNGMode` values in the *Reading Arm TrustZone RNG Configuration Parameters* code block.	*Arm TrustZone RNG Configuration Parameters*

Table B-3 Differences between issue 01 (v1.1) and issue 02 (v1.2)

Change	Location
Renamed TRNG driver modes.	Entire document
Minor rephrasing.	*Arm TrustZone RNG Overview*

Table B-4 Differences between issue 02 (v1.2) and issue 03 (v1.3)

Change	Location
Minor correction.	*Referenced Documents*
Rewritten.	*Introduction*
Added chapter.	*Chapter 1 Overview of Arm® TrustZone® TRNG* on page 1-8
Renamed from *ARM TrustZone RNG Overview* (added under *Overview*) and partially rewritten.	*Arm TrustZone RNG*
Renamed from *Characterization Overview*, and partially rewritten.	*RNG Characterization* on page 1-9
Merged *Characterization High-Level Procedure* into it and rewritten.	*Chapter 2 TRNG characterization procedure* on page 2-10
Renamed from *Setting the Output Files* and partially rewritten.	*2.3.1 Output-file names* on page 2-13

Table B-4 Differences between issue 02 (v1.2) and issue 03 (v1.3) (continued)

Change	Location
Added the section.	*2.2 Characterization test program* on page 2-12
Rewritten.	*2.3 Characterization test conditions* on page 2-13
Added the section, including the *Finding Minimum Sample Counter Value* code block moved from *First Characterization Iteration*.	*2.4 Base iteration* on page 2-14
Removed the section, and moved all its subsections under *Characterization Procedure*.	*Characterization Detailed Procedure*
Renamed from *First Characterization Test Program*, replaced first paragraph and removed step 1; partially rewritten.	*2.5 First characterization iteration* on page 2-15
Renamed from *Second Characterization Test Program*, and rewritten.	*2.6 Second characterization iteration* on page 2-16
Removed the section.	*Arm TrustZone RNG Configuration Parameters*

Table B-5 Differences between issue 03 (v1.3) and issue 04 (v1.4)

Change	Location
Renamed from *Introduction* and restructured.	*Preface* on page 0

Table B-6 Differences between issue 04 (v1.4) and issue 05

Change	Location
Template changes for the current releases.	Entire Document

Table B-7 Differences between issue 05 and issue 06

Change	Location
Document reclassified as Non-Confidential.	Entire document
Minor rephrasing in multiple sections. No technical changes.	Entire document
Split content into a new *2.1 Characterization procedure overview* on page 2-11 section. No technical changes.	*Chapter 2 TRNG characterization procedure* on page 2-10
Split content into a new *A.1 CC_TST_TRNG output format* on page Appx-A-18 section. No technical changes.	*Appendix A CC_TST_TRNG output* on page Appx-A-17