Application Processor Lite *ApP Lite*

TZ1000 Series

Reference Manual

MCU Random Number Generator

Revision 1.1

2018-02

TOSHIBA ELECTRONIC DEVICES & STORAGE CORPORATION

Table of Contents

List of Figures

List of Tables

Preface

This document provides the specification for the MCU Random Number Generator designed for the TZ1000 Series.

Intended Audience

This document is intended for the following users.

Driver software developers.

System designers

Conventions in this Document

- The following notational conventions apply to numbers:

Hexadecimal number:	0xABC
Decimal number:	123 or 0d123 (only when it should be explicitly indicated that the number is decimal)
Binary number:	0b111 (It is possible to omit the "0b" when the number of bit can be distinctly understood from a sentence.)

- Low active signals are indicated with a name suffixed with "_N".
- A signal is asserted when it goes to its active level while it is de-asserted when it goes to its inactive level.
- A set of multiple signals may be referred to as [m:n].
  Example: S[3:0] indicates four signals, S3, S2, S1 and S0, collectively.
- In the text, register names are enclosed in brackets ***[ ]***.
  Example:***[ABCD]***
- A set of multiple registers, fields or bits of the same type may be described collectively using "n".
  Example: ***[XYZ1], [XYZ2], and [XYZ3] to [XYZn]***
  A range of register bits are referred to as [m:n].
  Example: [3:0] indicates a range from bit 3 to bit 0.
- Values set in registers are indicated using either a hexadecimal or binary number.
- Example: ***[ABCD]***.EFG = 0x01 (hexadecimal), ***[XYZn]***.VW = 1 (binary)
- Words and bytes are defined as follows:

Byte:	8 bits
Halfword:	16 bits
Word:	32 bits
Doubleword:	64 bits

- Register bit attributes are defined as follows:

R:	Read-only
W:	Write-only
W1C:	Clear by write of 1 (a write of "1" clears the corresponding bit to 0)
W1S:	Set by write of 1 (a write of "1" sets the corresponding bit to 1)
R/W:	Read/Write
R/W0C:	Read/Clear by write of 0
R/W1C:	Read/Clear by write of 1
R/W1S:	Read/Set by write of 1
RS/WC:	Set by read/Clear by write (set after a read and cleared after a data write)

- Registers only support word access unless otherwise specified.
- Any registers defined as Reserved in the text must not be rewritten. Also, any values read from such registers should not be used.
- Any bits for which default values are defined as "-" would return undefined values if read.
- When a data is written to a register containing both writable and read-only (R) bit fields, its default values should be written to read-only (R) bit fields. For any bit fields with default values defined as "-", refer to the definitions of the relevant register.
- Default values should be written to any reserved bit fields in a write-only register. For any bit fields with default values defined as "-", refer to the definitions of the relevant register.

Abbreviation

These specifications introduce a part of the abbreviation which they used

RNG	Random Number Generator

1. Overview

The Random Number Generator (RNG) in this product generates 32-bit true random numbers.

2. Block Diagram

The block diagram of the RNG is shown in Figure 2.1. The RNG block consists of the RNG core which generates random numbers and the Bus I/F which is used to read the random numbers through the APB Bus.

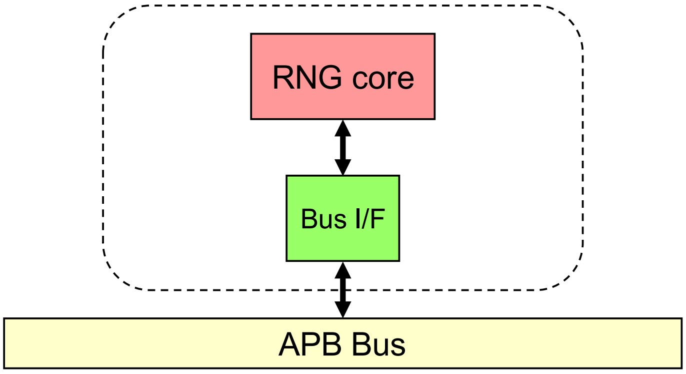

Figure 2.1 RNG block diagram

3. Address Map

Table 3.1 MCU Random Number Generator Register map

Register Name	Type	Width	Reset Value	Address Offset
RNDO	RO	32	0x0000 0000	0x0000 0000
RNDREADY	RO	32	0x0000 0000	0x0000 0004

4. Function

4.1. Clock and Reset

The RNG block clocks consists of the clock for the Bus I/F (rng_busclk) and the clock for the RNG core (rng_coreclk). Those clocks have the same frequency and are synchronized each other. Those clocks can be supplied to the blocks only when they are active, to save the power dissipation. And one reset signal synchronizes those clocks. The clocks and the reset are controlled by the PMU (Power Management Unit) outside of the RNG.

4.2. Power Management

The operation of each power mode is shown as follows.

- Sleep0: The random number generation is enabled. In other words, transition to this mode is enabled, when *[RNDREADY]*.RNDREADY is 0.
- Sleep1, Sleep2, WAIT/WAIT-RETENTION, and RETENTION: The random number generation is disabled because the RNG clocks stop. Before transition to these modes, the random number generation should be confirmed to stop by reading 1 from *[RNDREADY]*.RNDREADY. From this mode, the RNG returns to the mode before the transition.
- RTC and STOP: The random number generation is disabled because the RNG clocks stop. Before transition to this mode, the random number generation should be confirmed to stop by reading 1 from *[RNDREADY]*.RNDREADY. When returning from this mode, the RNG is initialized.

4.3. Start-up and Stop

4.3.1. Start-up Procedure

The RNG is in the following state when the power supply starts up.

- PE power supply domain where the RNG belongs: OFF state
- Clock supply: Stop
- Reset: Asserted

The RNG is enabled by the following procedure. The successive writes to the same register can be done at once.

- The following register should be read to confirm that the PE domain where the RNG belongs is supplied with power. For the power domain control, refer to Chapter 2 Power Management Unit
  - PMU *[POWERDOMAIN_CTRL_MODE]*.PDMODE_PE is confirmed to be 0b00.
- The bridge circuit for the RNG access is started up. For the start-up procedure of the bridge circuit, refer to Chapter 4 Bus Interconnect.
- The following register is set to supply the RNG with the clocks.
  - PMU *[CG_OFF_PE]*.CG_mpierclk_rng_coreclk is set to 1.
  - PMU *[CG_OFF_PE]*.CG_mpierclk_rng_busclk is set to 1.
- The following register is set to deassert the reset to RNG.
  - PMU *[SRST_OFF_PE]*.SRST_asyncrst_rng_rstn is set to 1.
- The following register is set to enable the dynamic clock gating for the RNG.
  - PMU *[DCG_PE]*.DCG_mpierclk_rng_coreclk is set to 1.
  - PMU *[DCG_PE]*.DCG_mpierclk_rng_busclk is set to 1.

4.3.2. Stop Procedure

When the RNG is not used, it is recommended to save the power dissipation that the reset is asserted and the power supply should be shut down. The stop procedure is as follows.

- *[RNDREADY]* .RNDREADY is confirmed to be 1.
- The following register is set to assert the reset to the RNG.
  - PMU *[SRST_ON_PE]*.SRST_asyncrst_rng_rstn is set to 1.
- The following register is set to stop the RNG clocks.
  - PMU *[CG_ON_PE]*.CG_mpierclk_rng_coreclk is set to 1.
  - PMU *[CG_ON_PE]*.CG_mpierclk_rng_busclk is set to 1.
- The power of the PE domain can be shut down. It is noted that the AESA in the domain also stops.

4.4. Frequency Setting

The RNG clock frequency can be changed by the setting of PMU *[PRESCAL_MAIN]*. PSSEL_CD_MPIER. The change can be done while the RNG is generating random numbers (*[RNDREADY]*.RNDREADY is 0).

4.5. Random Number Generation

The procedure of the random number generation is as follows.

(1) After deassertion of the reset, the random number generation is not done. *[RNDREADY]*.RNDREADY and *[RNDO]*.RNDO return 0.

(2) At 180 cycles after the reset deassertion, *[RNDREADY]*.RNDREADY becomes 1. A 6 Word random number is generated, and the number is read from *[RNDO]*.RNDO. However, it is recommended that the first 6 Word random number generated after the reset deassertion is not used because of low quality.

(3) After *[RNDO]*.RNDO is read 6 times, the next random number is generated. While it is generated, *[RNDREADY]*.RNDREADY and *[RNDO]*.RNDO are 0.

(4) After 180 cycles, *[RNDREADY]*.RNDREADY becomes 1. A new 6 Word random number is generated and it is read from *[RNDO]*.RNDO. The different Word of the 6 Words can be read when *[RNDO]*.RNDO is accessed successively. Then, 3. should repeat.

5. Details of Registers

5.1. RNDO

RNDO			
Description	Random Number Output Register		
Address Region	rng	Type:	RO
Offset	0x0000 0000		
Physical address View0	0x4002 1000		
Physical address View1	-		

Bitfield Details				
Bits	Name	Description	Access	Reset
31:0	RNDO	When [RNDREADY] is 1, 32-bit intrinsic random numbers can be read every time data is read. When [RNDREADY] is 0, 0 can be read. Although this is 0 immediately after reset cancellation, RNDREADY becomes 1 after a while, allowing random numbers to be read through this register.	RO	0x0000 0000

5.2. RNDREADY

RNDREADY			
Description	Random Number Ready Register		
Address Region	rng	Type:	RO
Offset	0x0000 0004		
Physical address View0	0x4002 1004		
Physical address View1	-		

Bitfield Details				
Bits	Name	Description	Access	Reset
31:1	Reserved	-	-	-
0	RNDREADY	0b0: 0 can be read through [RNDO] because of random numbers being generated. 0b1: Random numbers can be read through [RNDO] since random number generation has been completed. This is 0 immediately after reset cancellation, but becomes 1 after a while.	RO	0

6. Revision History

Table 6.1 Revision History

Revision	Date	Description
0.1	2014-04-02	Newly released
0.2	2014-04-04	Modified Start-up Procedure.
0.3	2014-06-25	Modified procedure of random number generation
0.4	2014-10-07	Modified random number generation time
0.5	2014-11-18	Modified Power Management
1.0	2015-01-23	Official version
1.1	2018-02-06	Changed header, footer and the last page. Changed corporate name and descriptions. Modified Arm logo and descriptions.

RESTRICTIONS ON PRODUCT USE

Toshiba Corporation and its subsidiaries and affiliates are collectively referred to as “TOSHIBA”.
Hardware, software and systems described in this document are collectively referred to as “Product”.

- TOSHIBA reserves the right to make changes to the information in this document and related Product without notice.
- This document and any information herein may not be reproduced without prior written permission from TOSHIBA. Even with TOSHIBA's written permission, reproduction is permissible only if reproduction is without alteration/omission.
- Though TOSHIBA works continually to improve Product's quality and reliability, Product can malfunction or fail. Customers are responsible for complying with safety standards and for providing adequate designs and safeguards for their hardware, software and systems which minimize risk and avoid situations in which a malfunction or failure of Product could cause loss of human life, bodily injury or damage to property, including data loss or corruption. Before customers use the Product, create designs including the Product, or incorporate the Product into their own applications, customers must also refer to and comply with (a) the latest versions of all relevant TOSHIBA information, including without limitation, this document, the specifications, the data sheets and application notes for Product and the precautions and conditions set forth in the "TOSHIBA Semiconductor Reliability Handbook" and (b) the instructions for the application with which the Product will be used with or for. Customers are solely responsible for all aspects of their own product design or applications, including but not limited to (a) determining the appropriateness of the use of this Product in such design or applications; (b) evaluating and determining the applicability of any information contained in this document, or in charts, diagrams, programs, algorithms, sample application circuits, or any other referenced documents; and (c) validating all operating parameters for such designs and applications. **TOSHIBA ASSUMES NO LIABILITY FOR CUSTOMERS' PRODUCT DESIGN OR APPLICATIONS.**
- **PRODUCT IS NEITHER INTENDED NOR WARRANTED FOR USE IN EQUIPMENTS OR SYSTEMS THAT REQUIRE EXTRAORDINARILY HIGH LEVELS OF QUALITY AND/OR RELIABILITY, AND/OR A MALFUNCTION OR FAILURE OF WHICH MAY CAUSE LOSS OF HUMAN LIFE, BODILY INJURY, SERIOUS PROPERTY DAMAGE AND/OR SERIOUS PUBLIC IMPACT ("UNINTENDED USE").** Except for specific applications as expressly stated in this document, Unintended Use includes, without limitation, equipment used in nuclear facilities, equipment used in the aerospace industry, medical equipment, equipment used for automobiles, trains, ships and other transportation, traffic signaling equipment, equipment used to control combustions or explosions, safety devices, elevators and escalators, devices related to electric power, and equipment used in finance-related fields. **IF YOU USE PRODUCT FOR UNINTENDED USE, TOSHIBA ASSUMES NO LIABILITY FOR PRODUCT.** For details, please contact your TOSHIBA sales representative.
- Do not disassemble, analyze, reverse-engineer, alter, modify, translate or copy Product, whether in whole or in part.
- Product shall not be used for or incorporated into any products or systems whose manufacture, use, or sale is prohibited under any applicable laws or regulations.
- The information contained herein is presented only as guidance for Product use. No responsibility is assumed by TOSHIBA for any infringement of patents or any other intellectual property rights of third parties that may result from the use of Product. No license to any intellectual property right is granted by this document, whether express or implied, by estoppel or otherwise.
- **ABSENT A WRITTEN SIGNED AGREEMENT, EXCEPT AS PROVIDED IN THE RELEVANT TERMS AND CONDITIONS OF SALE FOR PRODUCT, AND TO THE MAXIMUM EXTENT ALLOWABLE BY LAW, TOSHIBA (1) ASSUMES NO LIABILITY WHATSOEVER, INCLUDING WITHOUT LIMITATION, INDIRECT, CONSEQUENTIAL, SPECIAL, OR INCIDENTAL DAMAGES OR LOSS, INCLUDING WITHOUT LIMITATION, LOSS OF PROFITS, LOSS OF OPPORTUNITIES, BUSINESS INTERRUPTION AND LOSS OF DATA, AND (2) DISCLAIMS ANY AND ALL EXPRESS OR IMPLIED WARRANTIES AND CONDITIONS RELATED TO SALE, USE OF PRODUCT, OR INFORMATION, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY OF INFORMATION, OR NONINFRINGEMENT.**
- Do not use or otherwise make available Product or related software or technology for any military purposes, including without limitation, for the design, development, use, stockpiling or manufacturing of nuclear, chemical, or biological weapons or missile technology products (mass destruction weapons). Product and related software and technology may be controlled under the applicable export laws and regulations including, without limitation, the Japanese Foreign Exchange and Foreign Trade Law and the U.S. Export Administration Regulations. Export and re-export of Product or related software or technology are strictly prohibited except in compliance with all applicable export laws and regulations.
- Please contact your TOSHIBA sales representative for details as to environmental matters such as the RoHS compatibility of Product. Please use Product in compliance with all applicable laws and regulations that regulate the inclusion or use of controlled substances, including without limitation, the EU RoHS Directive. **TOSHIBA ASSUMES NO LIABILITY FOR DAMAGES OR LOSSES OCCURRING AS A RESULT OF NONCOMPLIANCE WITH APPLICABLE LAWS AND REGULATIONS.**

TOSHIBA ELECTRONIC DEVICES & STORAGE CORPORATION