

RNG4_ES ESV Public Use Document

Document Version 0.2

July 02, 2024

Copyright 2024 NXP Semiconductors - may be reproduced only in its original entirety (without revision)

Table of Contents

1 Description 3
2 Security Boundary 4
3 Operating Conditions 5
4 Configuration Settings 5
5 Physical Security Mechanisms 6
6 Conceptual Interfaces 6
7 Min-Entropy Rate 6
8 Health Tests 7
9 Maintenance 7
10 Required Testing 7

NXP Semiconductors Public Material – may be reproduced only in its original entirety (without revision)

1 Description

This document describes the design of the NXP RNG4_ES. The entropy source (depicted in Figure 1) is composed of a few major sections: the noise source and entropy estimator (health tests). This design uses either one ring oscillator as the Up Oscillator (in which case the system clock is used as the Down Oscillator) or two ring oscillators (in which case a rising edge of the Down Oscillator triggers the decrementing of the Down Counter). The general design of the ring oscillators consists of an inverting enabling gate and an even number of additional inverting delay elements formed into a ring. There is only one ring oscillators within all of the KW45 / K32W148 / MCX W71 designs covered by this Public Use Document.

This assessment was conducted using data and parameters measured in the evaluated version described In Table 1.

Table 1: Evaluated Entropy Source Specification

Identifier	Details
Entropy Source Name	RNG4_ES
Part Number	KW45 / K32W148 / MCX W71
Hardware Revision	A2
Entropy Category	Physical (P)
Test Platform(s)	KW45 / K32W148 / MCX W71
Entropy Estimation Track (per SP 800-90B §3.1.2)	Non-IID

When used to seed an SP 800-90A DRBG, the seeding requirements listed in the table below must be met.

DRBG Security Strength	Bits Required to Instantiate (Random Nonce)	Bits Required to Instantiate (Nonce Provided)
128-bit	235	157
192-bit	352	235
256-bit	470	313

Copyright NXP Semiconductors 2024

NXP Semiconductors Public Material – may be reproduced only in its original entirety (without revision)

2 Security Boundary

The RNG4_ES noise source is depicted in block diagram below.

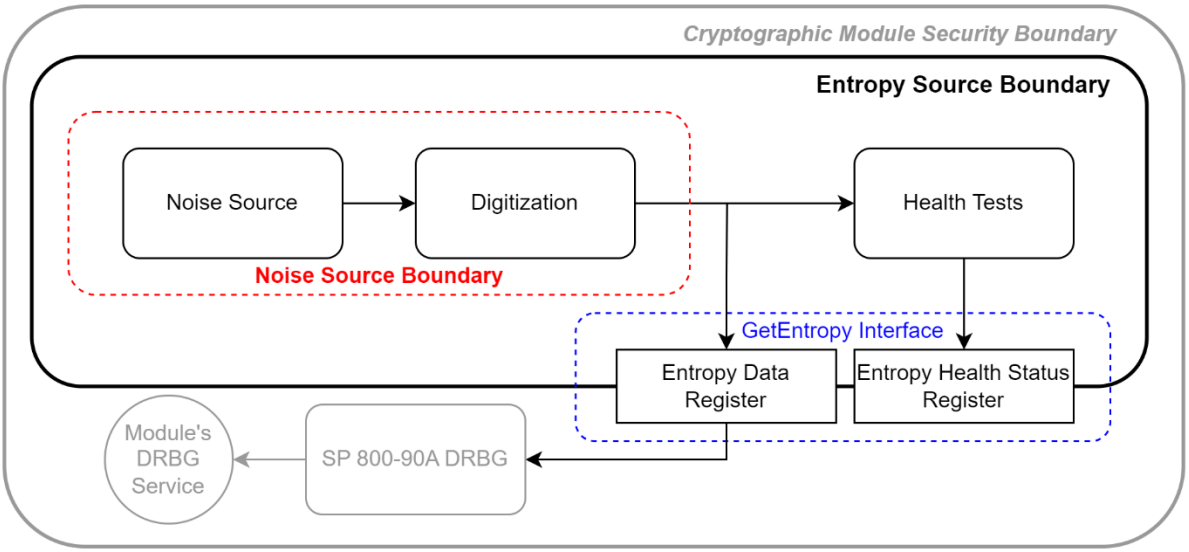


Figure 1: RNG4 entropy source

NXP Semiconductors Public Material – may be reproduced only in its original entirety (without revision)

3 Operating Conditions

The Entropy-relevant operating conditions are given in Table 2.

Table 2: Entropy-Relevant Operating Conditions

Parameter	Value
Temperature	-40C to 105C
Voltage	1.05V to 1.15V (Core)

4 Configuration Settings

All entropy-relevant parameters must be verified as set as specified in Table 3.

Table 3: Entropy-Relevant Configuration Parameters

Parameter	Value	Description
Entropy Delay	1500	Ring oscillator cycle count corresponding to a single bit of entropy per the [EAR].
von Neumann Post Processing	Disabled	Enable or disable Von Neumann post-processing.
Health Test Bounds	As described in Table 4	See Table 4
Health Test Retries Allowed	1	Number of attempts to retry health testing.
Ring Oscillator Clock Divider	0	A provision to slow the ring oscillator rate; unused.
Downclock Source	System Clock	Sample clock source selector.
Statistical Test Block Size	512	Number of bits generated and tested by the self-tests.

Table 4: Health test bounds

	Min	Max
Bits tested = 512		
Monobit Test	195	317
Poker Test	0.8	72.1
Runs of length 1	27	107
Runs of length 2	7	62
Runs of length 3	0	39
Runs of length 4	-1	26
Runs of length 5	-1	18
Runs of length 6+	-1	17
Long runs		32

Copyright NXP Semiconductors 2024

NXP Semiconductors Public Material – may be reproduced only in its original entirety (without revision)

5 Physical Security Mechanisms

The RNG4_ES entropy source operates within the physical protections of the associated SoC package, a commercial plastic ball grid array package. In addition, the NXP SoC devices are mounted onto PCBs, protecting access to the ball grid array.

6 Conceptual Interfaces

The RNG4_ES provides entropy data to the cryptographic module in which it is implemented, and this module is considered to be the user of the entropy source. The process of using the GetEntropy() interface is the process of reading the Entropy Data Register, and this interface is only provided to the user of the entropy source.

7 Min-Entropy Rate

The min-entropy rate for the output of the RNG4_ES is 0.818696 bits/bit.

Copyright NXP Semiconductors 2024

NXP Semiconductors Public Material – may be reproduced only in its original entirety (without revision)

8 Health Tests

The RNG4_ES implements the health tests with NXP recommended bounds as follows:

Table 4. Health Tests and NXP Recommended Bounds

Health Test	512-bit Block	
	Min	Max
Monobit Test	195	317
Poker Test	0.8	72.1
Runs of length 1	27	107
Runs of length 2	7	62
Runs of length 3	0	39
Runs of length 4	-1	26
Runs of length 5	-1	18
Runs of length 6+	-1	17
Long runs		32

If a generated block of entropy data fails the self-test, the design can be configured to discard the data and generate a new block of data to be tested. A re-try counter (see the *Health Test Retries Allowed* configuration parameter) is used to specify how many times data should be discarded before signaling an error.

9 Maintenance

The RNG4_ES design does not require maintenance.

10 Required Testing

The RNG4_ES as incorporated in the KW45 / K32W148 / MCX W71 family was tested by collected data from the device operating in its designated operational range and processed with the SP 800-90B tool. Test data was collected following the requirements of Section 3 of SP 800-90B. No additional testing is required by the end user.

Copyright NXP Semiconductors 2024

NXP Semiconductors Public Material – may be reproduced only in its original entirety (without revision)