RNG4 ESV Public Use Document

Document Version 0.1

July 14, 2023

Table of Contents

References

Ref.	Full Specification Name	Date
[90A]	NIST, SP 800-90A Rev. 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators	24-Jun-2015
[90B]	NIST, SP 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation	10-Jan-2018
[140IG]	NIST, Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program	4-May-2021
[ESVMM]	Entropy Source Validation, program Management Manual (under development)	TBD
[EAR]	Keypair Consulting Inc., "NXP RNG4 Entropy Analysis and SP800-90B Compliance Report	10-Mar-2022

1 Description

This document describes the design of the NXP RNG4 entropy source (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 are two ring oscillators within all of the RW61x designs covered by this Public Use Document.

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

Table 1: Evaluated Entropy Source Specification

Identifier	Details
Entropy Source Name	RNG4_ES
Part Number	rpp_cm0p_sec_subsys
Hardware Revision	A2
Firmware Version	MCUXpresso Integrated Development Environment (IDE) v11.7.1_9221
Entropy Category	Physical (P)
Test Platform(s)	RW610 and RW612
Entropy Estimation Track (per SP 800-90B §3.1.2)	Non-IID

The entropy source provides entropy input to a [90A] compliant DRBG implemented in hardware.

2 Security Boundary

The RNG4_ES noise source is depicted in block diagram below.

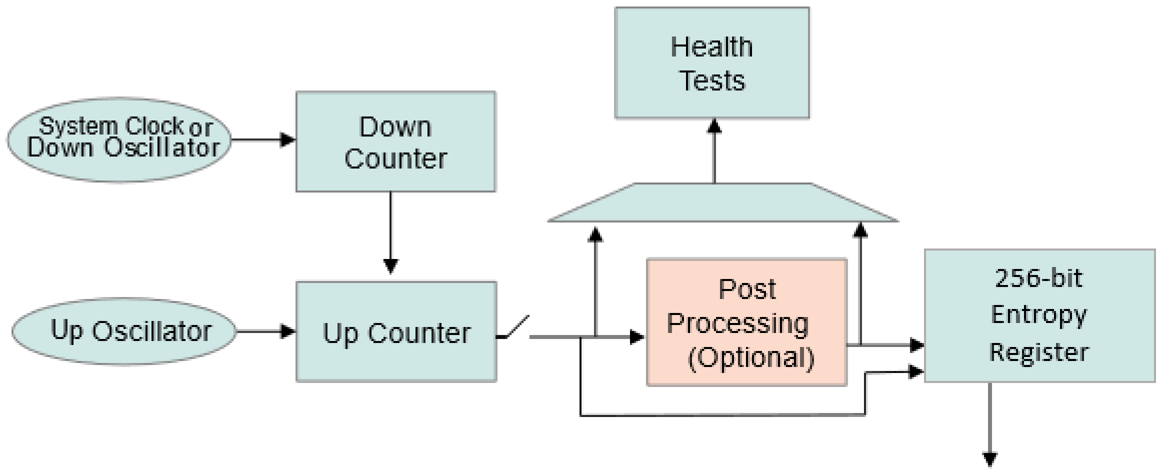

Figure 1: RNG4 entropy source

3 Operating Conditions

The Entropy-relevant operating conditions for all entropy source variants listed in Table 1 are given in Table 2.

Table 2: Entropy-Relevant Operating Conditions

Parameter	Value
Temperature	-40C to 85C
Voltage	0.955V to 1.115V (Core)

4 Configuration Settings

All entropy-relevant parameters (I.e., operating conditions) must be set as specified in Table 3.

Table 3: Entropy-Relevant Configuration Parameters

Parameter	Value	Description
Entropy Delay	15000	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	OSC2	Sample clock source selector.
Statistical Test Block Size	1024	Number of bits generated and tested by the self-tests.

Table 4: Health test bounds

	Min	Max
Bits tested = 1024		
Monobit Test	427	596
Runs of length 1	75	187
Runs of length 2	28	105
Runs of length 3+	33	97
Long runs		32

5 Physical Security Mechanisms

The NXP RNG4 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 as incorporated in the RW610 family of SoCs is fully self-contained. The conceptual interface is provided as a service of the secure enclave subsystem within the SoC as well as the use of random bits as required to fulfill other secure enclave services.

7 Min-Entropy Rate

The min-entropy rate for the RNG4 TRNG is 207 bits per 256 bits or 0.809743 bits/bit.

8 Health Tests

The RNG4 implements the health tests with NXP recommended bounds as follows:

Table 4. Health Tests and NXP Recommended Bounds

Health Test	1024-bit Block		512-bit Block	
	Min	Max	Min	Max
Monobit Test	427	596	196	316
Run Length 1	75	187	28	107
Run Length 2	28	105	8	62
Run Length 3	33	97	10	55
Long Runs		32		<=31

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 (*Health Test Retries Allowed)* is used to specify how many times data should be discarded before signaling an error.

9 Maintenance

The RNG4 design does not require maintenance.

10 Required Testing

The RNG4 as incorporated in the RW61x families 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.