SP 800-90B Non-Proprietary Public Use Document

Entropy Source Name: STM32U535x/545x TRNG

Document Version: 1.1

Hardware Version: revision Z

STMicroelectronics
12 rue Jules Horowitz
38000 Grenoble, Isere
France

May 05, 2025

Revision History

Version	Change
1.0	Initial version
1.1	Correct configuration with Bit 12 of RNG_CR set (see Table 2) Update PUD to NIST V1.2 PUD template with “User Verification” and “Vendor Permissions and Relationship” sections added

Table of Contents

Description 4
Security Boundary 4
Operating Conditions 5
Configuration Settings 5
Physical Security Mechanisms 6
Conceptual Interfaces 7
Min-Entropy Rate 7
Health Tests 7
Maintenance 7
User Verification 8
Vendor Permissions and Relationship 8

Description

The STM32U535x/545x TRNG entropy source is the physical hardwired peripheral generating random numbers, implemented in the STM32U535x/545x family of microcontrollers of revision Z.

The version of the STM32U535x/545x TRNG entropy source can be read as 0x41 from the version register in the RNG peripheral (RNG_VERR).

This entropy source was evaluated in compliance with NIST SP800-90B from Jan. 2018 and FIPS 140-3 Implementation Guidance from Dec. 2024. The tests were performed using the NIST SP800-90B Entropy Assessment Test Suite in version 1.1.8.

Security Boundary

The STM32U535x/545x TRNG entropy source depicted in Figure 1 below, is composed of a few major sections, which map to the conceptual components contained within an SP 800-90B entropy source.

The STM32U535x/545x TRNG entropy source contains:

- Physical noise source, consisting of multiple copies of an analog noise source following SP 800-90B and FIPS 140-3 IG D.K Resolution 10.
- Digitization
- Health tests including:
  - Startup
  - On-Demand
  - Continuous
- AES-128 CMAC Conditioning

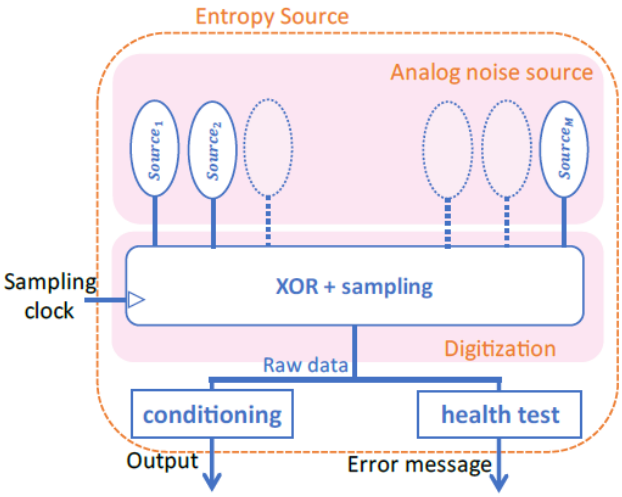


Figure 1: The STM32U535x/545x TRNG Entropy Source

The analog noise sources are dedicated to the entropy source peripheral, and their behaviors cannot be altered by any code or by any debugger.

Operating Conditions

Table 1 summarizes the operating conditions under which the STM32U535x/545x TRNG source entropy assessments have been performed.

Parameter	Value	Description
System clock	160 MHz	Microprocessor CPU clock
Temperature	25 °C	Microprocessor operating temperature range
RNG AHB clock	160 MHz	RNG peripheral bus clock
RNG kernel clock	48 MHz	RNG peripheral dedicated kernel clock (integrated oscillator HSI)
MCU digital voltage Vdd	1.8V or 3.3V	MCU main digital power supply Vdd. Range1 (VCORE = 1.2 V) with CPU and peripherals running at up to 160 MHz. Internal regulator automatically set VCORE to 1.2v when MCU digital voltage Vdd is 1.8V or 3.3V

Table 1: Operating Conditions

Configuration Settings

To operate as a compliant entropy source, the entropy source shall be configured according to the settings specified below in Table 2 (sample interval, start-up delay, conditioning function and compression ratio, health-tests cut-off). For more information, refer to the ‘RNG operation’ and ‘RNG registers’ sections of the RNG chapter in the product reference manual.

Register	Description	Bits	Values	Comment
RNG_CR	Control register	[31:0]	0x80F1 1FXX	This configuration is valid for RNG Kernel clock= 48MHz. By setting bit 31, the application can lock the RNG configuration until next IP reset. The XX value depends on the application: • Bit 2 is set when RNG peripheral is needed • Bit 5 is set to detect too low RNG kernel clock • Bit 3 is set to enable RNG interrupts. Other bits in the byte stays at 0.
RNG_NSCR	Noise source control register	[31:0]	0x0000 24C2	This register is used to activate mutually independent sources.
RNG_HTCR	Health test register	[31:0]	0x0000 76B3	F α=2^{-20} corresponds to C=29 for the RCT and C=691 for the APT.

Table 2: Entropy Source Register Configurations

The RNG_HTCR controls the health test cutoffs for the SP 800-90B approved health tests. The option in the table above, α=2^{-20}, represents the selection of a false positive rate for the entropy source health tests to operate with. This is achieved by the register selecting different cutoff limits for each health test, which has been mathematically calculated to have the respective false positive rate.

Physical Security Mechanisms

The STM32U535x/545x TRNG entropy source is a fully hardwired module implemented in the microcontroller's integrated circuit as an RNG peripheral. The entropy source module does not give access to raw data from the noise source (see *Conceptual Interfaces*).

The STM32U535x/545x microcontroller hardware and software resources can be partitioned so that they exist either in the secure world or in the non-secure world, using Arm® TrustZone® technology. The secure world can be used to protect critical code against intentional or unintentional tampering from the more exposed code running in the non-secure world. The initial partitioning of the platform is under the responsibility of the secure firmware executed after reset of the device. This protection is activated when TZEN option bit is set in the FLASH_OPTR register.

The STM32U535x/545x TrustZone® hardware protection can be used to protect the configuration of the RNG peripheral, to ensure the correct behavior of the entropy source. Specifically, application can set RNGSEC bit in GTZC1_TZSC_SECCFGR3 register to restrict access to the RNG peripheral to the secure world only. Setting this bit also restricts to secure world only the RNG peripheral control bits for clock, reset, clock source selection and clock enable during low-power modes.

Conceptual Interfaces

The GetNoise interface is available for certification purposes only. Indeed, when using microcontrollers dedicated to entropy certification, the entropy source can provide the raw data generated by the noise source, by reading the RNG peripheral data register (RNG_DR). The raw data of the noise source is never available when using standard STM32U535x/545x microcontrollers.

The GetEntropy interface is accessible in the field. The entropy source provides 128 bits of random data outputted by the conditioner in the RNG peripheral data register (RNG_DR). When the entropy is collected from the RNG_DR register, the user must verify that the bit 2 of the RNG_SR register (SECS) is not set. If it is set, the random data must not be used, and the recovery sequence described in the 'Error management' section of the RNG chapter in the product reference manual must be followed.

The HealthTest interface is always accessible. The entropy source clears the bit 2 of RNG status register (RNG_SR) if the entropy source passed the NIST SP800-90B approved health tests. The bit 2 is set otherwise.

Min-Entropy Rate

The STM32U535x/545x TRNG entropy source provides 128 bits of min-entropy per 128 bits output sample, or full entropy. The 128 random bits result from 4 successive readings of the RNG_DR register, which contains 32 bits of random data.

Health Tests

The STM32U535x/545x TRNG entropy source continuously performs the repetition count test (RCT) and the adaptative proportion test (APT) Health Tests specified in SP800-90B section 4.4. The health tests operate at a false positive rate of $\alpha=2^{-20}$.
On-demand health tests can be initiated by restarting the entropy source.

Maintenance

No maintenance is required for the STM32U535x/545x TRNG entropy source.

User Verification

No further verification from the user is required. The user must check a correct configuration of the entropy source and rely on the health tests to ensure that the device is operating correctly.

Vendor Permissions and Relationship

The ESV certificate for the STM32U535x/545x TRNG entropy source “Open for Reuse”, meaning any vendor can use the certificate within their module without any specific permission.