SP 800-90B Non-Proprietary Public Use Document

Entropy Source Name: STM32U59x/5Ax TRNG

Document Version: 1.2

Hardware Version: revision X and later

STMicroelectronics
39 Chemin du Champ des Filles
Plan-Les-Ouates, Geneva, CH-1228
Switzerland

March 25, 2024

Revision History

Version	Change
1.0	Initial version
1.1	Table 1 updated
1.2	Updated Required Testing section.

Table of Contents

Description

The STM32U59x/5Ax TRNG entropy source (referenced as STM32U5x TRNG in this document) is the physical hardwired peripheral generating random numbers, implemented in the STM32U59x/5Ax family of microcontrollers of revision B and Later.

Version of the STM32U5x TRNG entropy source can be read as 0x41 from the version register in the RNG peripheral (RNG_VERR).

Security Boundary

The STM32U5x 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 STM32U5x 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
- Conditioning

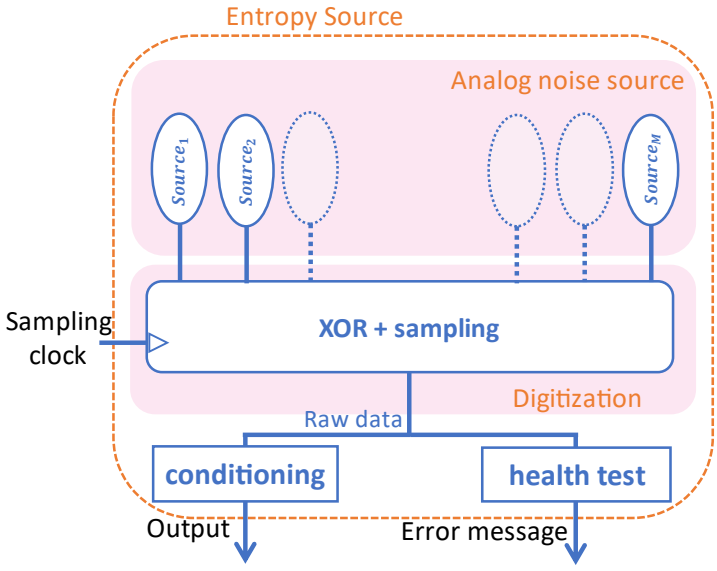

Figure *1*: The STM32U5x TRNG Entropy Source

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 STM32U5x 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

When using the register configurations summarized in Table 2, the STM32U5x TRNG entropy source configuration is set correctly (sample interval, startup delay, conditioning function and compression ratio, health-tests cutoffs).

Register	Description	Bits	Values	Comment
RNG_CR	Control register	[31:0]	0x80F10FXX	This configuration is valid for RNG Kernel clock= 48MHz. Bit 31 locks 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, and bit 3 is set to enable RNG interrupts. Other bits in the byte stays at 0.
RNG_NSCR	Noise source control register	[31:0]	0x00001609	This register is used to activate mutually independent sources.
RNG_HTCR	Health test register	[31:0]	0x000092F3	For $\alpha=2^{-20}$ corresponds to 36 for repetition tests and 755 for adaptive tests

Table 2: Entropy Source Registers Configurations

The RNG_HTCR controls the health test cutoffs for the SP 800-90B approved health tests. The option in the table above, $\alpha=2^{-20}$, 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 STM32U5x 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.

The STM32U59x/5Ax 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 STM32U59x/5Ax TrustZone® hardware protection can be used to protect the configuration of the RNG peripheral and to ensure the correct behavior of the entropy source. Specifically, the application can set the RNGSEC bit in GTZC1_TZSC_SECCFGR3 register to restrict access to the RNG peripheral to 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.

RNG peripheral 48MHz clock source (HSI48) configuration can also be made secure-only in the RCC peripheral.

Conceptual Interfaces

The GetNoise interface is available for certification purpose 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 STM32U59x/5Ax microcontrollers.

The GetEntropy interface is accessible in the field. The entropy source provides random data outputted by the conditioner directly in the RNG peripheral data register (RNG_DR).

The HealthTest interface is always accessible. The entropy source clears to 0 the bits 1 & 2 of RNG status register (RNG_SR) if the entropy source passed the NIST SP800-90B approved health tests. The bits 1 & 2 are set to 1 otherwise.

Min-Entropy Rate

The STM32U5x TRNG entropy source provides 128 bits of min-entropy per 128 bits output sample, or full entropy.

Health Tests

The STM32U5x 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 false positive rate of $\alpha=2^{-20}$.

Maintenance

No maintenance is required for the STM32U5x TRNG entropy source.

Required Testing

Built-in Health Tests described in the Health Tests section constantly check the validity of the noise source. No further testing is required.