CRYPTO4A

SP 800-90B Non-Proprietary Public Use Document
Crypto4A QASM Entropy Source

Firmware Version: v1.0
Hardware: QASM v1.0 (Xilinx ZYNQ Ultrascale+)

Crypto4A Technologies, Inc.
1550A Laperriere Avenue
Ottawa, ON K1Z 7T2

October 30, 2023

Document Version 1.0

Revision History

Version	Date	Change
0.1	October 16, 2023	Initial draft.
1.0	October 30, 2023	Final submission for ENT to ESV Conversion.

Table of Contents

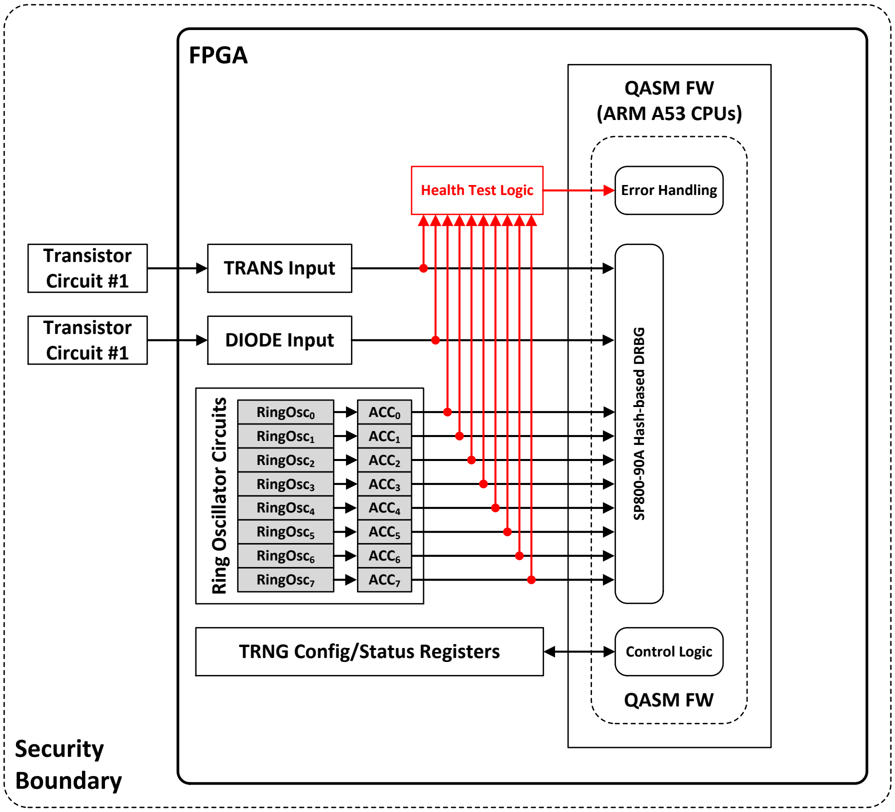
Description

The Crypto4A QASM Entropy Source is a physical entropy source. It makes no IID claim and thus meets all requirements for non-IID compliance.

Security Boundary

The security boundary of the Crypto4A QASM Entropy Source is shown in the figure below. This boundary includes the analog noise sources (i.e., internal ring oscillator-based entropy source circuits and the two external transistor-based entropy sources), the digitization circuitry, the online health test logic, and the ACC conditioning function. In addition, though not shown, it includes entropy FIFO logic which provides observability of the raw entropy samples from each of the noise sources, including the outputs of the ring oscillators prior to the ACC conditioning function, for entropy characterization and measurement.

All of the outputs are used by the QASM firmware running on the embedded ARM A53 processing cores to seed an SP 800-90A compliant DRBG.



Operating Conditions

The Crypto4A QASM Entropy Source is claimed to operate correctly over the following operating environments and condition ranges:

Hardware	Supply Voltage	Temperature
QASM v1.0 (Xilinx ZYNQ Ultrascale+)	0.81V to 0.89V	0C to 40C

Configuration Settings

The Crypto4A QASM Entropy Source configuration and status registers allow for fine-grained control over various aspects of the entropy generation process, as described by the detailed register map below.

The various sample rate and threshold registers have default values that are automatically loaded at power-on reset so the QASM firmware does NOT need to configure any settings in order to start the entropy generation and self-checking process. The firmware need only be concerned with monitoring the results of the self-checking process and handling any error conditions that may arise from it.

Name	Access	Purpose/Function
AXI_TRNG_CNTRL	RW	Provides control of the TRNG-related logic. Bit [28] enables the TRNG's operation and generation of new random values. Setting this bit to 1 will transition the TRNG from the DISABLED to the ENABLED state (see AXI_TRNG_STATUS). Setting this bit to 0 will force the TRNG into the DISABLED state which will zero all TRNG-related data outputs. This bit is automatically cleared upon start of either a startup or on-demand health test. Bit [24] sets the TRNG's operating mode (0 = normal operation, 1 = test mode that drives entropy FIFO). Bit [20] Initiates a self-test cycle on-demand. The TRNG will disable its data outputs and enter the TESTING state, where it will remain until the self-tests are completed and reported in AXI_TRNG_TEST_STATUS. Bit [16] flushes the entropy FIFO when set to a 1, and the HW will self-clear the bit when it has completed the flush. Bits [2:0] select the entropy FIFO's source using the mappings: 0 = raw ring oscillator output 1 = ring oscillator ACC conditioning logic output 2 = TRANS noise source 3 = DIODE noise source
AXI_TRNG_STATUS	RO	Reports the status of TRNG-related logic. Bit [31] indicates if the TRNG startup test has completed (1 = test completed, 0 = test still ongoing). Bits [30:28] indicate the current state of the TRNG's top level FSM which controls the behaviour of the TRNG logic. The

Name	Access	Purpose/Function
		possible values, and their corresponding state descriptions are: 0 = IDLE (TRNG is currently in reset) 1 = TESTING (TRNG is currently executing either a startup or on-demand test operation and its data outputs are zeroed. 2 = DISABLED (TRNG is currently disabled and its outputs are zeroed) 3 = ENABLED (TRNG is operating normally) Bits `[7:0]` indicate whether AXI_TRNG_DATA[7:0] registers have been read since they were last updated (i.e., bit `[3]` = 0 indicates AXI_TRNG_DATA3 hasn't been updated since it was last read, bit `[3]` = 1 indicates AXI_TRNG_DATA3 has been updated with new random data so it can be sampled safely). Bit `[8]` provides the aforementioned status functionality for the output of the TRANS noise source input register. Bit `[9]` provides the aforementioned status functionality for the output of the DIODE noise source input register.
AXI_TRNG_ROSC_CNTR	RW	Bits `[15:0]` are used to set a sample rate counter for when the TRNG's ring oscillator will be updated in terms of clock periods (e.g., `[15:0]` = 0xFFFF indicates that the TRNG's free-running output will be sampled every 65535 clock periods).
AXI_TRNG_ACC_CNTR	RW	Same basic principle as AXI_TRNG_ROSC_CNTR but this controls the sample rate of the TRNG's ACC conditioning logic (e.g., `[15:0]` = 0x1000 indicates that the TRNG's ACC logic will be updated every 4096 clock periods).
AXI_TRNG_DATA0	RO	Bits `[31:0]` of TRNG's 256-bit output.
AXI_TRNG_DATA1	RO	Bits `[63:32]` of TRNG's 256-bit output.
AXI_TRNG_DATA2	RO	Bits `[95:64]` of TRNG's 256-bit output.
AXI_TRNG_DATA3	RO	Bits `[127:96]` of TRNG's 256-bit output.
AXI_TRNG_DATA4	RO	Bits `[159:128]` of TRNG's 256-bit output.
AXI_TRNG_DATA5	RO	Bits `[191:160]` of TRNG's 256-bit output.
AXI_TRNG_DATA6	RO	Bits `[223:192]` of TRNG's 256-bit output.
AXI_TRNG_DATA7	RO	Bits `[255:224]` of TRNG's 256-bit output.
AXI_TRANS_CNTR	RW	Same basic principle as AXI_TRNG_ROSC_CNTR but this controls the sample rate of the transistor-based TRANS noise input (e.g., `[15:0]` = 0x2000 indicates that the TRANS input will be sampled every 8192 clock periods).
AXI_TRANS_DATA	RO	Bits `[31:0]` of TRANS input register.

Name	Access	Purpose/Function
AXI_DIODE_CNTR	RW	Same basic principle as AXI_TRNG_ROSC_CNTR but this controls the sample rate of the transistor-based DIODE noise input (e.g., `[15:0]` = 0x4000 indicates that the DIODE input will be sampled every 16384 clock periods).
AXI_DIODE_DATA	RO	Bits `[31:0]` of DIODE input register.
AXI_ENTROPY_STATUS	RO	Bit `[16]` indicates if the entropy capture FIFO has filled, and this bit remains stuck at one until this register is read (which causes the bit to be cleared), thereby allowing you to see if you've missed capturing entropy samples due to the FIFO overflowing since you last checked. Bits `[12:0]` indicate the current entropy capture FIFO depth (i.e., number of entropy samples currently stored in the FIFO).
AXI_ENTROPY_DATA	RO	Reading this register returns the current output of the capture FIFO and triggers the logic to read the next element from the FIFO so that it is ready-and-waiting for the next read of this register.
AXI_TEST_CNTRL	RW	Bit `[9]` enables the background online testing of the DIODE data inputs (1 = DIODE data tested continuously). Bit `[8]` enables the background online testing of the TRANS data inputs (1 = TRANS data tested continuously). Bits `[7:0]` enable the background online testing for the 8 ring oscillator data inputs used to feed the ACC conditioning logic.
AXI_TEST_ROSC_TCFG	RW	Bits `[31:16]` specify the threshold used for the adaptive proportion test running on the 8 ring oscillator data inputs. Bits `[15:0]` specify the threshold used for the repetition count test running on the 8 ring oscillator data inputs.
AXI_TEST_TRANS_ TCFG	RW	Same idea and bit-mapping as AXI_TEST_ROSC_ TCFG, but for the online tests performed on the TRANS data input.
AXI_TEST_DIODE_ TCFG	RW	Same idea and bit-mapping as AXI_TEST_ROSC_ TCFG, but for the online tests performed on the DIODE data input.
AXI_TEST_STATUS	RW	Reports either the current state of the online adaptive proportion and repetition count tests (in the ENABLED state), or the result of the last startup/on-demand test that was executed (in the DISABLED state). Bit [25] indicates result of the adaptive proportion test on the DIODE data input (1 = failed, 0 = passed). Bits [24:16] represent the same sort of information as bit [25], but for the TRANS, ROSC[255:192], …, ROSC[31:0] respectively.

Name	Access	Purpose/Function
		Bit [9] indicates the result of the repetition count test on the DIODE data input (1 = failed, 0 = passed). Bits [8:0] represent the same sort of information as bit [9], but for the TRANS, ROSC[255:192], …, ROSC[31:0] respectively.

Physical Security Mechanisms

The Crypto4A QASM Entropy Source is enclosed entirely within the module's cryptographic boundary, which is protected by tamper evident seals, anti-probing barriers, environmental monitors, and is assessed for FIPS 140-2 level 3 Physical Security compliance.

Conceptual Interfaces

The noise, entropy, and online health test results are provided via dedicated pins/registers from the Crypto4A QASM Entropy Source so there is no real conceptual interface at this level of the design. The QASM firmware utilizes these physical interfaces to implement the logical functions GetEntropy and HealthTest by interacting with the aforementioned registers to deliver the desired functionality.

Min-Entropy Rate

The measured min entropy per output sample of the ring oscillator noise source with non-vetted ACC conditioner is 239.878912 bits per 256-bit output.

Health Tests

The Crypto4A QASM Entropy Source implements the NIST SP 800-90B (section 4) Repetition Count Test (RCT) and Adaptive Proportion Test (APT) health tests, which are run at start up and continuously during operation. There is a unique instance of each health test logic block for each entropy source within the device, and each instance has its own set of status flags to inform the QASM firmware of the validity of the corresponding entropy source. The default test thresholds are set to have a false positive rate of 2^{-30}, as specified in Section 4.3 of SP 800-90B.

Any detected failures will trigger a response by the QASM firmware to attempt to reset the failing entropy source, blocking access to its output so long as it remains in the failed state (and while it is being re-tested). If all entropy sources are in the failed state when the DRBG goes to reseed using the outputs of the Crypto4A QASM Entropy Source then the QASM firmware will enter an error state which prevents it from being able to perform any operations that require it to generate random data using the DRBG. In this error state the operator will be forced to reset the platform to attempt to correct the operation of the Crypto4A QASM Entropy Source .

Maintenance

There are no maintenance requirements specific to the entropy source.

Required Testing

The target platform testing included gathering 1,000,000 raw data samples as well as 1,000 samples of raw data after each of 1,000 restarts. No additional testing is required.

The health tests can be initiated on demand to verify that the entropy source is configured and operating correctly using the following procedure:

1. Set bit 20 of the AXI_TRNG_CNTRL register to ‘1’.
2. Monitor the AXI_TRNG_STATUS register until bits [30:28] indicate the DISABLED state which indicates the health test has completed.
3. Read the AXI_TEST_STATUS register to ascertain the results of the health test (an all-zero value indicates no failures).
4. If all is well, re-enable the TRNG by setting bit 28 of the AXI_TRNG_CNTRL register to ‘1’.