Intel DRNG SP800-90B Non-Proprietary Public Use Document

Intel DRNG Entropy Source

Document Version : 1.2

Design Version :
DRNG4.2_PIC6_V1, RNG_ES_GEN3.0

David Johnston
dj.johnston@intel.com

Intel Corporation

2200 Mission College Blvd,

Santa Clara,

CA 95054

Table of Contents

1 Description

The Intel DRNG (Digital Random Number Generator) Entropy Source is a physical (P) entropy source.

The circuit component is RNG_ES_GEN3.0

The synthesizable RTL component is DRNG4.2_PIC6_V1. All components of the entropy source are hardware, consisting of logical and electronic components bounded in a rectangle of silicon. There is no firmware or software within the entropy source.

The entropic data from the entropy source is non-IID.

This PUD is applicable to the following products referred to collectively as FM7:

Intel® Agilex™ F-Series AGF 019 FPGAs and SoC FPGAs
Intel® Agilex™ F-Series AGF 023 FPGAs and SoC FPGAs
Intel® Agilex™ I-Series AGI 019 FPGAs and SoC FPGAs
Intel® Agilex™ I-Series AGI 023 FPGAs and SoC FPGAs

Table 1 List of Applicable Devices

The devices listed above all use the same die and package. The only difference between them is how they are fused. The fusing defines which components outside the DRNG are turned on/off depending on the customer's price point. The DRNG itself is static silicon that is the same for all the devices listed above.

2 Security Boundary

The DRNG security boundary surrounds the set of components referred to as the DRNG core, that includes the Digital Noise Source, CHTs (Continuous Health Tests), AES-CBC-MAC Vetted Conditioning Component, DRBG, NRBG, and register interface. The security boundary is a sub boundary within the DRNG. Components outside the security boundary but within the DRNG are to attach to the local bus, clock, and power systems on the chip. The DRNG security boundary is not a FIPS140 security boundary. It is designed to be usable within a larger FIPS140 security boundary through compliance to SP800-90A, B and draft C along with relevant requirements in ISO/IEC 19790-2012 and FIPS140-3. The red rectangle outline in Figure 1 shows the boundary of the entropy source, the black bold outline in Figure 1 is the security boundary of DRNG, which includes the entropy source and other DRNG components.

For use as a full entropy source, the NRBG output of the DRNG is the necessary output. The NRBG output path to the regio block is the output of the full entropy source, as an RBG3 construction in the draft SP800-90C. The DRBG output path to the regio block is the output of the DRBG, as an RBG2 construction. The NRBG construction is the XOR construction from Draft SP800-90C. This XORs the output of the conditioner with an output from the DRBG for the NRBG output. The width of these

operations is 128 bits, driven by the output size of AES. The registers sizes are 64 bits, and in the logic, this width transforming is performed using a FIFO that is 64 bits wide and takes in 128 bits as two 64-bit entries and outputs 64 bits to match the register width.

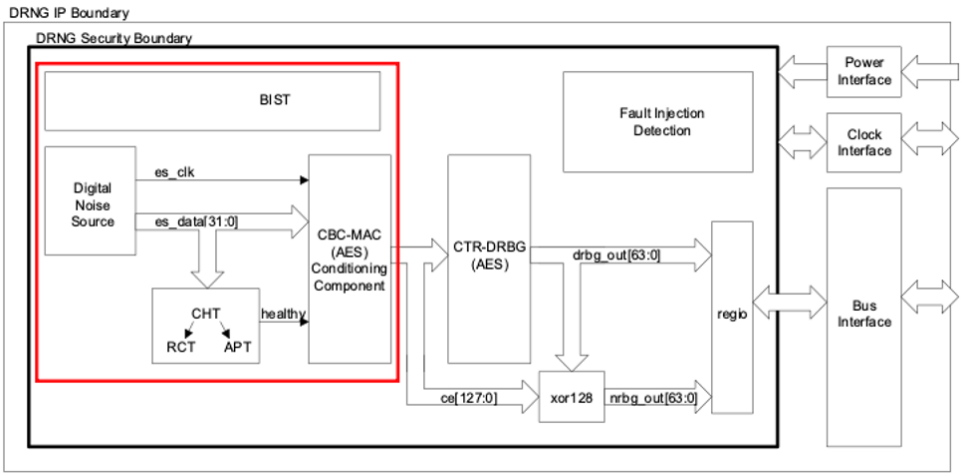

Figure 1 DRBG Security Boundary

In the context of FM7, the DRNG register that presents the NRBG output to the local bus is called EGETDATA. The result is passed to the target register of the instruction and the success or failure signaled in the carry flag.

This report is applicable to the devices in Table 1. The silicon manufacturing process, IC design and DRNG design is identical for each of these devices. Differences between these devices are the set of enabled features, which has no influence on the DRNG behavior.

3 Operating Conditions

The entropy source is guaranteed to operate within the designated operating range defined in this document. In Intel® Agilex™ F-Series and I-Series the operating envelope is as follows in Table 2:

Parameter	Minimum	Maximum
Temperature	-25C	90C
Voltage	0.8V – 5%	0.8V + 5%
Clock frequency	~1.6GHz	~1.6GHz

Table 2 Operating Conditions

4 Configuration Settings

There are no configuration settings accessible at any privilege level to firmware running in FM7.

5 Physical Security Mechanisms

The DRNG contains several physical security mechanisms that are built into the logic within the security boundary. Specifically:

Sparse Coding

> A mechanism where n-bit representations of values are mapped to m-bit representations where m > n. An algorithmic search was done to maximize the hamming distance between the encoded representations. A received value not in the set of valid representations will trigger an alarm. This is a general defense against fault injection attacks.

Arc Integrity

> In each state of each state-machine within the security boundary, the state from which the current state was visited is checked against the list of valid states that can reach the current state. If the arc integrity check is violated, an alarm will be triggered. This is a defense against fault injection attacks that aim to push a state machine into a state it would otherwise not be in.

SBOX Masking

> SBOX masking is implemented in the AES engine. Being in hardware, the randomly generated masks are fixed. Each SBOX has a different mask. This is a basic defense against side channel attacks against SBOX emissions.

Consistency Checks

> There are various conditions in the DRNG. Test modes, operation modes, buffer states, state machine states etc. There are many cases where particular combinations of these states should not exist simultaneously. For example, a test mode should not be enabled when the DRNG is operating in its normal and secure mode. Several consistency checks are implemented and if one of these checks fails, an alarm will be triggered.

When an alarm is triggered, the DRNG resets itself and re-runs BIST. It is not possible to distinguish between a failure due to attack or environmental bounds violation or a rare false positive error. The re-running of BIST will lead to the DRNG failing if the BIST fails. In the case of a transitory error, the DRNG will recover when BIST is re-run.

The packaging of the chip is a tamper evident enclosure.

6 Conceptual Interfaces

GetEntropy(n) is used to get a random number, where n can be one of 16, 32 or 64, depending on the size of the target register.

7 Min Entropy Rate

Figure 2 illustrates the required min-entropy rate and the actual observed min-entropy rate of the noise source and the chain of conditioners consisting of a non-vetted XOR Feedback Decorrelator-Decimator and a vetted AES-CBC-MAC. The XOR Feedback Decorrelator-Decimator is a digitizer per design, but for the sake of 90B compliance, it is treated as a non-vetted conditioner.

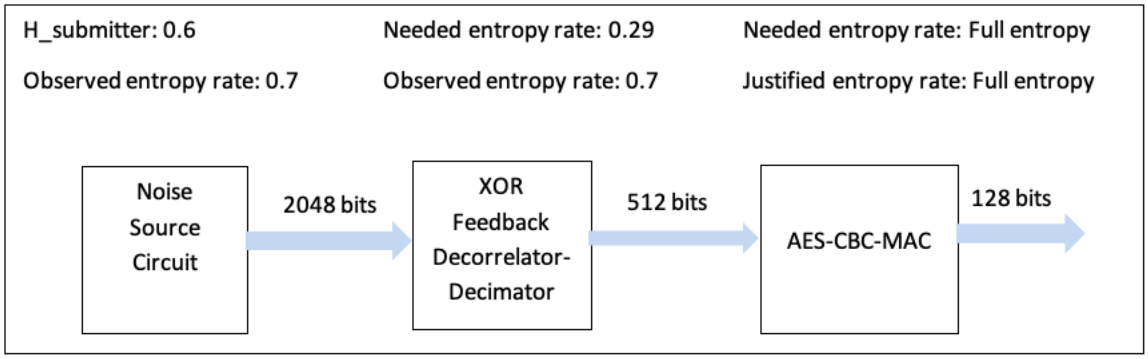

Figure 2 Entropy Levels on Noise Source and Conditioning Chain

The output of the AES-CBC-MAC conditioner has the full entropy, given that the input to the AES-CBC-MAC has an entropy rate that is greater than 0.29. The ≥0.29 entropy rate requirement from the digitized noise source is based on the SP 800-90B section 3.1.5.1.1 equation for the minimum input entropy requirement of the vetted AES-CBC-MAC conditioner.

The 0.6 entropy rate on the pre-digitizer data is a design target across all variants of silicon. The actual observed entropy rate on the noise source prior to digitization on FM7 is greater than 70%. The digitization stage does not reduce the entropy rate, and it is observed that the entropy rate of the post-digitizer data feeding into the AES-CBC-MAC conditioner is greater than 0.7. The difference between the 0.29 and 0.7 entropy rates is the engineering margin in the design of the entropy source.

8 Health Tests

The DRNG includes

Continuous Health Tests (CHTs)

Startup Noise Source Health Tests

Startup Logic Integrity BIST

The vendor defined Continuous Health Test is composed of a short-term test yielding a pass/fail over individual 256 bit blocks of noise source data and a long term evaluation of the pass/fail history of the past 256 block (totaling 65536 bits) to infer an entropy source failure. The failure condition is invoked when the pass rate drops below 50%.

The logic integrity test is one of the startup tests. This performs a test of the digital logic by running deterministic random sequences through all the logic and testing the resulting output against the expected result.

The Startup Noise Source Health Test involves running the CHTs for a probationary period of 65536 bits from the noise source. When the test is complete, assuming the test passes, the RNG enters the operational state. This happens during FM7 startup and completes before the first instructions can execute. The startup test is invoked at power-on or exiting the reset state. So, the startup tests can be invoked by power cycling or resetting FM7.

A failure in any of the startup tests (logic integrity or noise source health test) will be reflected as a BIST failure in the internal status register which leads to an MCHECK failure.

Following the startup tests, the CHTs continue to run. Should failure condition of the CHT test be encountered after the startup tests have completes, this may be either the result of a soft error or a hard error. The test will continue to run and should the entropy quality return, it will exit the failure state. In the failure state, no more random numbers are issued, and the failure state is reflected in the BIST status register result bits. Should some condition exist (E.G., out of specification operating condition), cessation of that condition will lead to resumption of the supply of random numbers.

9 Maintenance

There are no maintenance action requirements.

10 Required Testing

Raw noise testing was performed using the Non_IID lower bound entropy tests of the SP800-90B Entropy Assessment software tool, showing the entropy from the noise source to exceed the minimum input threshold H_I of 0.29 of the vetted conditioning component.

Restart testing was performed using the SP800-90B Entropy Assessment software tool, showing the startup min entropy of H_r and H_c to be greater than 50% of H_I.

11 Legal Notices and Disclaimers

Intel provides these materials as-is, with no express or implied warranties.

All products, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice.

Performance varies by use, configuration, and other factors. Learn more at www.Intel.com/PerformanceIndex

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure.

Performance results are based on testing as of 2022-04-18 and may not reflect all publicly available security updates. See configuration disclosure for details. No component or product can be absolutely secure.

Some results have been estimated or simulated using internal Intel analysis or architecture simulation or modeling and provided to you for informational purposes. Any differences in your system hardware, software or configuration may affect your actual performance.

Intel and the Intel logo are trademarks of Intel Corporation in the United States and other countries.

Code names are used by Intel to identify products, technologies, or services that are in development and not publicly available. These are not "commercial" names and not intended to function as trademarks.