Microsemi Corporation
One Enterprise Way
Aliso Viejo, CA 92656

US: (800) 713-4113
Int: (949) 380-6100
Fax: (949) 215-4996

Microsemi White Paper

EnforcIT® RNG Core Randomness Quality

Power and Microelectronics Group
West Lafayette Division
Version 1.0

February 2014

Introduction

The security of systems implementing cryptography are highly dependent on quality random numbers. Without a quality random number generator modern crypto systems could not generate keys required to cryptographically secure sensitive date. Microsemi’s EnforcIT® product is a set of IP cores written in VHDL aimed at protecting sensitive FPGA designs and data from attack. To augment the EnforcIT Cryptography Suite, a Random Number Generation (RNG) IP core is provided, emitting high quality and NIST compliant random numbers to an FPGA design. *This white paper will describe the quality of randomness found in Microsemi’s EnforcIT Cryptography Suite, specifically the RNG core.*

RNG Structure

The Random Number Generator IP Core (RNG) in the EnforcIT® Cryptography Suite is implemented based on the ANSI X9.82 and NIST SP800-90 standards. RNG implements an entropy whitening function by using AES in counter mode to provide backtracking/prediction resistance. The RNG is composed of two primary components:

1) An internal non-deterministic random bit generator (source) and
2) A deterministic random bit generator (AES-CTR DRBG, whitening).

To ensure the entropy source is of a high quality, additional steps are taken to remove bias and localized correlation. A continual health check is run to look for statistical deviations from “randomness”. These steps all occur at runtime.

Quality

Additional testing is performed in a lab setting. Using the target device of choice, random data is collected on the entropy source and collected post conditioning. This random data is analyzed using the NIST SP800-22rev1a, “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications”, test suite. This test suite contains RNG tests that use a theoretical random distribution to determine pass/fail criteria for the collected data. These tests include items such as the monobit test (# of 1s and 0s), runs test (long runs of a data set), DFT testing, and so on. The tests use the reference distribution to determine an appropriate decision rule for the P-value. The P-value is used to assess the strength of the evidence against the null hypothesis (that the sequence being test is random) to determine the proportion of tests that should pass.

Conclusion

Due to the statistical nature of RNG analysis, verification of RNG quality is not an exact science. Fifteen NIST tests are run in the suite. Microsemi’s RNG IP core passes all NIST tests reliably with the exception of the non-overlapping template test. After deep investigation, it was discovered that reference random data sets from the DIEHARD suite and random.org also fail the test in a statistically indistinguishable manner.

All EnforcIT IP cores, including RNG, were developed in a US-only facility by cleared US citizens. They are EAR99 export controlled and are immediately ready for deployment in Xilinx, Altera, and Microsemi FPGAs.

About Microsemi

Microsemi Corporation (NASDAQ: MSCC) offers a comprehensive portfolio of semiconductor and system solutions for communications, defense & security, aerospace and industrial markets. Products include high-performance, radiation-hardened and highly reliable analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and voice processing devices; RF solutions; discrete components; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services.

Microsemi's security portfolio includes FPGAs, SoCs, cryptography solutions, encrypted solid state drives, intellectual property, firmware and other scalable anti-tamper products. The company also offers a comprehensive suite of security-related services, as well as design, assembly, packaging and testing services.

Microsemi is headquartered in Aliso Viejo, Calif., and has approximately 3,000 employees globally. Microsemi maintains a DMEA accredited facility in Phoenix, Ariz. for assembly and test and a U.S. only facility in West Lafayette, Ind. Its quality and inspection system requirements are certified to MIL-PRF-38534 Class H and K, MIL-PRF-38535 Class Q, ISO 9001:2008 and AS9100. For more information call (800) 713-4113 or visit www.microsemi.com.