Highlights

-

Overview

The security strength of many systems and applications is dependent on the quality of random number generators. Many cryptographic operations require a source of random numbers, such as the creation of cipher keys and initial values for counters and protocol parameters.

The DesignWare® True Random Number Generator (TRNG) Core for NIST SP 800-90c is compliant with NIST SP 800-90A/B/c and BSI AIS 20/31 specifications. It generates random numbers that are statistically equivalent to a uniformly distributed data stream. The core includes a NIST SP 800-90B The DesignW

implementations to be validated with NIST SP 800-22 specified tests and certified under Federal Information Processing Standards, FIPS 140-2 and FIPS 140-3. The core implementation is compatible with standard digital standard cell processes and can easily be tuned for a specific target library/process, including the most advanced nodes such as 5nm.

The DesignWare TRNG Core for NIST SP 800-90c block diagram in Figure 1 shows the noise source sending a noise stream to the conditioning component to produce full-entropy seed that is then fed into the DRBG to generate random numbers. A health-test block is included to perform Known Answer Tests (KAT) and various statistical tests required by NIST SP 800-90A/B/c and BSI AIS 20/31 standards. The health-test block is capable of performing start-up, on-demand, and continuous tests.

Deliverables

- Verilog HDL developed in compliance with the IEEE 1364 Verilog-2005 standard
-