True Random Number Generator for NIST SP 800-90c

Highlights

- NIST "Live, Enhanced NRBG"
- Compliant with NIST SP 800-90A/B/c, AIS 20/31, FIPS 140-2 and FIPS 140-3
- Designed for compliance with OSCCA certification
- Customer configurable
- Area: 60+ K ASIC gates
- Performance: up to 3.2 Gbps at 500 MHz
- Wide system clock dynamic range
- Virtualization support (up to 8 TRNGs)
- Selectable number of seed generators: 6 or 8
- Background raw noise collection for fast reseeding
- Redundant internal seed generators
- Continuous statistical and on demand known answer health tests
- Serial output stream for auxiliary uses
  - Differential power analysis
  - Timing analysis
- Interfaces
  - Memory mapped (AXI/AHB/APB)
  - Serial random bit streams (up to 3)
  - Nonce interface compatible with DesignWare HDCP Content Protection ESMs

Target Applications

- Security protocols
- Networking
- Mobile
- Consumer electronics
- IoT
- Automotive
- Government/military

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 approved conditioning circuit with a compliant noise source and NIST SP 800-90A approved Deterministic Random Bit Generator (DRBG) using the terminology preferred by the National Institute of Standards and Technology (NIST). The noise source does not depend on process-specific circuitry and is therefore very portable across different ASIC and FPGA fabrication technologies. When implemented in silicon, the DesignWare TRNG can meet or exceed the highest commercial and US government SBU standards.

DesignWare True Random Number Generator IP for NIST SP 800-90c

The DesignWare TRNG Core for NIST 800-90c is designed to be used in 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.

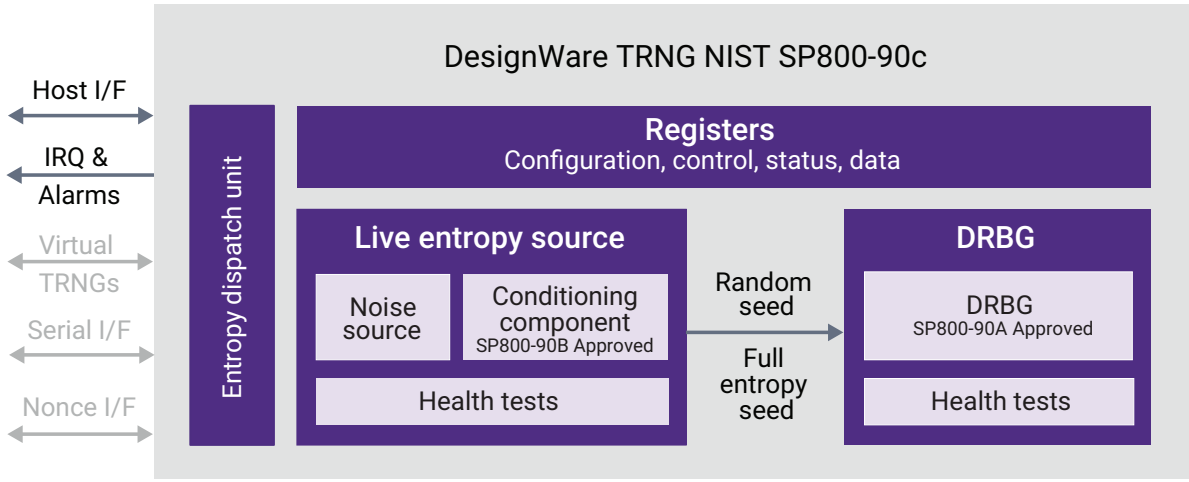

Figure 1: DesignWare TRNG IP for NIST SP

The DesignWare TRNG Core for NIST SP 800-90c can generate random seeds from the internal ring-oscillator-based noise source or can be manually seeded via a host provided nonce. A host-provided nonce will be fed into the conditioning component to increase the entropy rate using a NIST SP 800-90B approved conditioning function. If the host's nonce has enough entropy, the nonce can also be directly loaded into the DRBG to be used as a seed.

Random number generators are ultimately dependent on the physical implementation of seed generator, the manufacturing process, and other physical characteristics of the overall design. Therefore, full compliance testing of RTL-based semiconductor IP to the listed standards is not possible. Synopsys' TRNG IP has been implemented and utilized in numerous semiconductor designs of which several of these designs have undergone FIPS 140-2 and NIST Cryptographic Module Validation Program (CMVP) compliance testing.

The TRNG core can be reseeded from the ring-oscillator based seed generator or can be manually reseeded via a host defined nonce. When multi-channel support option is enabled, a reseed reminder alarm indicates that to the host that the current seed is tale and should be refreshed.

The core has a register mapped memory interface which can be configured to support AMBA AXI, AHB, or APB. A serial interface is available to support up to 3 bit streams if a direct hardware based random serial stream is required (e.g. for Differential Power Analysis side channel countermeasures support). A parallel nonce interface compatible with HDCP 2.x Content Protection Embedded Security Modules is also available.

The DesignWare TRNG Core for NIST SP 800-90c can operate for a wide system clock dynamic range, from ~30MHz all the way up to the maximum frequency achievable in the system, making it feasible to support significantly different operating frequencies (e.g 30+MHz during boot up and 1+GHz during runtime).

The TRNG core has the option to include virtual TRNGs which provides the ability to access random numbers securely between multiple readers such as in a multi-core processor system (up to 8 virtual TRNGS are supported). Each register interface which provides random numbers has a clear on read which prevents number re-use.

As noise collection is a slow process because of its non-deterministic nature, the TRNG core supports background noise collection. Using this mode, new entropy can be generated in the background and stored for the next seeding operation to eliminate the wait time for the next reseeding.

Other Synopsys Security IP

- DesignWare True Random Number Generator IP – "Live, Conditioned Digitized Noise Source"

Deliverables

- Verilog HDL developed in compliance with the IEEE 1364 Verilog-2005 standard
- Testbench and test vectors
- Sample synthesis script and constraints
- Sample simulation script
- Documentation
- Reference software development kit (SDK)

About DesignWare IP

Synopsys is a leading provider of high-quality, silicon-proven IP solutions for SoC designs. The broad DesignWare IP portfolio includes logic libraries, embedded memories, embedded test, analog IP, wired and wireless interface IP, security IP, embedded processors, and subsystems. To accelerate prototyping, software development and integration of IP into SoCs, Synopsys' IP Accelerated initiative offers IP prototyping kits, IP software development kits, and IP subsystems. Synopsys' extensive investment in IP quality, comprehensive technical support and robust IP development methodology enable designers to reduce integration risk and accelerate time-to-market.

For more information on DesignWare IP, visit synopsys.com/designware.