TRNG1

True Random and Pseudorandom Number Generator Core

General Description

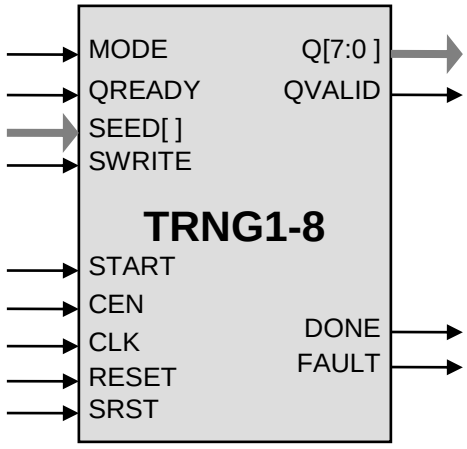
The true random generator core implements true random number generation. The core passes the American NIST Special Publication 800-22 and Diehard Random Tests Suites. It is compliant with FIPS 140-2 Annex C.

Basic core is very small (8,000 gates) and contains the random seed source and a PRNG1 cryptographically secure pseudo-random generator core.

The design is fully synchronous, with the exception of the seed part, and available in both source and netlist form.

The core is supplied as portable Verilog (VHDL version available) thus allowing customers to carry out an internal code review to ensure its security.

Symbol



Base Core Features

Satisfies Federal Information Processing Standard (FIPS) Publication 140-2 Annex C (“approved” random number generator) from the US National Institute of Standards and Technology (NIST). Passes the requirements of the NIST SP 800-22.

High security (128 bit entropy; 256 version available)

Initial seed provided from internal entropy source

Automatic re-seeding

High data rate

Completely self-contained: does not require external memory

Available as fully functional and synthesizable Verilog.

Deliverables include synthesis scripts

Applications

Secure wireless communications, including IEEE 802.16 WiMAX, 802.11 Wi-Fi WLAN, 802.15.3, 802.15.4 (ZigBee), MBOA, 802.16e

Electronic financial transactions, smart cards

Content protection, digital rights management (DRM), set-top boxes

Secure video surveillance systems

Military communication systems

Encrypted data storage

Secure RFID

Pin Description

Name	Type	Description
CLK	Input	Core clock signal
CEN	Input	Synchronous enable signal. When LOW the core ignores all its inputs and all its outputs must be ignored.
MODE	Input	When HIGH, the START will initiate a pseudo-random generate operation based on the initial seed (normal mode). When LOW, the START going high will force a true random re-seed (external entropy can also be applied via the SEED input).
START	Input	Starts the core operation
RESET	Input	Asynchronous core reset
SRESET	Input	Synchronous core reset
QREADY	Input	External circuitry is ready for the data
DONE	Output	Indicates the completion of a re-seed or generate operation
Q[ ]	Output	Output of pseudorandom data
QVALID	Output	Core is driving valid data on the Q bus
SEED[ ]	Input	Input of seed data. Ignored in the normal mode.
SVALID	Input	Seed data is valid
FAULT	Output	Internal seed source is not operational

Function Description

TRNG1 can be operated in two modes: forced re-seeding and normal. During the normal operation, asserting START causes the core to output the random numbers on its Q output. The numbers are produced by the random number generator based on internal entropy source and the data on the SEED input. Re-seeding in the normal mode occurs automatically.

In the forced re-seeding mode the internal entropy source is directly used to generate the random numbers.

Available Versions

The TRNG1 core is available in with different datapath widths and throughputs.

Export Permits

US Bureau of Industry and Security has assigned the export control classification number 5E002 to the AES1 core inside TRNG1. The core is eligible for the license exception ENC under section 740.17(A) and (B)(1) of the export administration regulations. See the IP Cores, Inc. licensing basics page, http://ipcores.com/exportinformation.htm, for links to US government sites and more details.

Deliverables

HDL Source Licenses

- Synthesizable Verilog RTL source code
- User Documentation

Contact Information

IP Cores, Inc.
3731 Middlefield Rd.
Palo Alto, CA 94303, USA
Phone: +1 (650) 815-7996
E-mail: info@ipcores.com
www.ipcores.com