BERTEN
Secure Communications

TRNG-P201 IP Core

Physical True Random Number Generator

High Throughput

Robust Entropy Source

Low Resource Utilisation

Background contains a copiable example of a raw random sequence generated with the IP Core

Features

- High-quality Entropy Source
- AIS-31 PTG.2 Compliant
- FIPS 140-3 Compliant
- NIST 800-90B Health Tests
- Passes NIST SP800-22 Test Suite
- Passes Diehard Battery of Tests
- Internal Fault Detection
- Portable to any FPGA or ASIC
- AMBA-AXI Interface

Applications

- Secure Communications
- Encrypted Data Storage
- Cryptographic Protocols
- User Authentication
- Electronic Transactions
- Noise Generation

The TRNG-P201 IP core generates reliable physical true random sequences for any FPGA, SoC, or ASIC design targeting cryptographic applications. The non-deterministic entropy source is based on multi-phase oscillators, producing a high-quality RNG. The core is optimised for low resource utilisation.

The IP Core is compliant with NIST 800-90B, FIPS 140-3, and AIS-31 PTG.2 standards. It provides the raw random sequence, or a post-processed output obtained from a configurable parity filter.

Portable to any AMD (Xilinx), Intel (Altera), or Microchip (Microsemi) device, the RNG passes NIST 800-22, AIS-31, and Diehard test suites. Operation is continuously monitored, triggering alarms when fault conditions are detected.

TRNG-P201 includes AMBA-AXI interfaces and a register map with user-programmable parameters to configure the output rate, parity filter, health tests, and alarms management.

www.bertendsp.com sales@bertendsp.com +34 942 18 10 11

Entropy Source

The non-deterministic entropy source is sampled at the input clock frequency to generate true random bits. The maximum rate of the random sequence depends on the target device.

The raw output can be post-processed using a XOR parity filter with a configurable length up to 128 bits.

Performance

In the following table, resource utilisation and maximum raw sequence output rate for different speed grades (SP), are provided. Additional details and metrics for other devices are available as required. Placement constraints are applied to ensure timing closure after integration into customer design.

	Device Family	LUT	Register	Output Rate (SP)
AMD / Xilinx	Spartan-7	2.5K	2.3K	212 Mbps (1) 270 Mbps (2)
	Artix-7 (*)	2.5K	2.3K	212 Mbps (1) 270 Mbps (2)
	Kintex-7, Virtex-7 (*)	2.5K	2.3K	320 Mbps (1) 405 Mbps (2)
	Kintex/Virtex Ultrascale	2.5K	2.3K	415 Mbps (1) 461 Mbps (2)
	Artix/Kintex/Virtex Ultrascale+ (*)	2.5K	2.3K	575 Mbps (1)
	Versal ACAP	2.2K	2.3K	575 Mbps (1)
Intel	MAX 10	4.1K	1.7K	130 Mbps (7)
	Cyclone 10 LP	4.1K	1.7K	130 Mbps (7)
	Cyclone V	2.7K	1.9K	211 Mbps (7) 241 Mbps (6)
	Arria 10	2.7K	1.8K	300 Mbps (3) 373 Mbps (2)
	Stratix V	2.8K	1.8K	486 Mbps (1)

(*) *Also applicable to Zynq SoC*

Interfaces

The TRNG provides the entropy source or the parity filter output through an AXI4-Stream interface.

The core includes a register map with a complete set of user-programmable parameters to configure the output rate, parity filter, health tests thresholds, and alarms behaviour. Access to registers is implemented using an AXI4-Lite interface.

Health Tests

The TRNG-P201 includes the following configurable health tests:

- Total failure of the Entropy Source and Known-Answer Tests (KAT) according to AIS-31.
- Repetition Count and Adaptive Proportion according to NIST 800-90B.
- Monobit and Runs tests according to NIST 800-22.

Health tests trigger alarms when fault conditions are detected. It is possible to specify which critical warnings disable the output data.

Licensing

The IP Core is provided as encrypted netlist for one device family, under a perpetual Site Licence. It includes 12 months of maintenance and remote support for the integration of the TRNG core in your platform.

Deliverables

- Targeted, timing closed Netlist
- Design Constraints and Scripts
- User Manual
- ANSI C drivers for register map configuration