BERTEN Digital Signal Processing

TRNG-P200 IP Core

Physical True Random Number Generator

High Throughput

Robust Entropy Source

Register-based Configuration

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

Features

- High-quality Entropy Source
- Passes AIS-31 PTG.2 Test Suites
- NIST SP800-22 Compliant
- NIST 800-90B & AIS-31 Health Tests
- FIPS 140-2 Compliant
- 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-P200 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 in a minimum area.

The IP core provides simultaneously the raw random sequence, and two post-processed outputs obtained from a parity filter and a configurable polynomial encoder.

Portable to any Xilinx, Intel, or Microsemi device, TRNG-P200 passes NIST 800-22, AIS-31 PTG.2, and Diehard test suites.

The core implements a complete set of health tests compliant with NIST 800-90B, FIPS 140-2, and AIS-31. Operation is continuously monitored, triggering alarms when fault conditions are detected.

TRNG-P200 includes AMBA-AXI interfaces and a register map with user-programmable parameters to configure the output rate, polynomial encoder, health tests, and alarms management. ANSI C drivers implementing this register-based configuration are available for integration in the target platform.

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 raw random sequence depends on the target device.

The raw output is post-processed using a 2-bit XOR parity filter, and a configurable polynomial encoder with predefined BCH codes.

Performance

In the following table, resources utilisation and maximum raw sequence output rate for different speed grades (SP), are provided. Additional details and metrics for any Xilinx, Intel, or Microsemi FPGA or SoC are available as required. Placement constraints are applied to ensure timing closure after integration into customer design.

	Device Family	LUT	Register	Output Rate (SP)
Xilinx	Spartan-7	4.7K	5.0K	212 Mbps (1) 270 Mbps (2)
	Artix-7 (*)	4.7K	5.0K	212 Mbps (1) 270 Mbps (2)
	Kintex-7, Virtex-7 (*)	4.7K	5.0K	320 Mbps (1) 405 Mbps (2)
	Kintex/Virtex Ultrascale	4.6K	5.0K	415 Mbps (1) 461 Mbps (2)
	Kintex/Virtex Ultrascale+ (*)	4.6K	5.0K	575 Mbps (1)
Intel	MAX 10	7.6K	4.5K	130 Mbps (7)
	Cyclone 10 LP	7.6K	4.5K	130 Mbps (7)
	Cyclone V	5.3K	4.8K	211 Mbps (7) 241 Mbps (6)
	Arria 10	5.4K	4.7K	300 Mbps (3) 373 Mbps (2)
	Stratix V	5.5K	4.7K	486 Mbps (1)

(*) *Also applicable to Zynq SoC*

Interfaces

The TRNG provides raw and post-processing output sequences through AXI4-Stream interfaces.

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

Health Tests

TRNG-P200 implements a complete set of configurable health tests, including:

- Total failure of the Entropy Source and Known-Answer tests according to AIS-31.
- Repetition Count and Adaptative Proportion according to NIST 800-90B.
- Monobit, Frequency Test within a Block, Longest Run of Ones in a Block, Overlapping Template Matching, Cumulative Sums, and Runs test according to NIST 800-22.
- Continuous Random Number Generator test according to FIPS 140-2.

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