BERTEN
Secure Communications

DRBG-C301 IP Core

Deterministic Random Bit Generator

AES-based Security
Register-based Configuration
Block-cipher Derivation Function

Features

- Based on AES-256 in Counter Mode
- Block-cipher Derivation Function
- Prediction Resistance and Reseeding
- AIS-20 DRG.4 Compliant
- NIST SP 800-90A Compliant
- Portable to any FPGA or ASIC
- FIPS 140-3 Compliant
- Internal Fault Detection
- AMBA AXI Interfaces

Applications

- Secure Communications
- Network Security: MACsec, IPsec
- Cryptographic Protocols
- User Authentication
- Electronic Transactions
- Noise Generation

The **DRBG-C301** generates deterministic random numbers for any FPGA, SoC, or ASIC design targeting cryptographic applications. The IP core is based on the NIST CTR_DRBG mechanism using AES-256 Counter mode.

The DRBG-C301 is compliant with NIST SP 800-90A and AIS-20 DRG.4 standards, and it can be combined with a high-quality entropy source to achieve compliance with NIST SP 800-90C RBG3 and AIS-31 PTG.3.

The IP Core supports prediction resistance and reseeding functionalities and accepts both Personalization String and Additional Input parameters.

Portable to any AMD (Xilinx), Intel (Altera), or Microchip (Microsemi) device, the IP core is also compliant with FIPS 140-3 and provides the highest performance in a minimum area.

DRBG-C301 includes AMBA AXI interfaces and a user-programmable register map to configure the generation of random bits. ANSI C drivers are provided for a fast integration into the target platform.

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

Deterministic Random Bit Generator

DRBG-C301 implements a Bit Generator and a Derivation function using AES-256 encryption.

The Derivation Function processes arbitrary-length data (seed material) to output a fixed-length string. The result is transferred to an optimised Bit Generator that produces the deterministic random bits.

Performance

Resource utilisation for different devices is provided in the table below. Metrics for other FPGA and SoC are available as required.

The DRBG-C301 generates up to 9 random bits per clock cycle (2.7 Gbps @300 MHz).

	Device Family	LUT	Register
AMD / Xilinx	7 Series	2.5K	2.6K
	Ultrascale	2.4K	2.6K
	Ultrascale+	2.4K	2.6K
	Versal ACAP	2.5K	2.5K
Intel / Altera	MAX 10, Cyclone 10 LP	5.8K	2.5K
	Cyclone V	2.4K	2.5K
	Arria 10	2.4K	2.5K
	Stratix V	2.4K	2.5K

Interfaces

The DRBG implements two AXI4-Stream interfaces for high-speed data transfer. One AXI4-Lite provides access to the register map for configuration and control. Alarms and Status notifications are available through dedicated ports.

Health Tests

DRBG-C301 includes a complete set of Known-Answer tests that are executed at power-up or after a reset. An alarm is triggered if a failure is detected.

Licensing

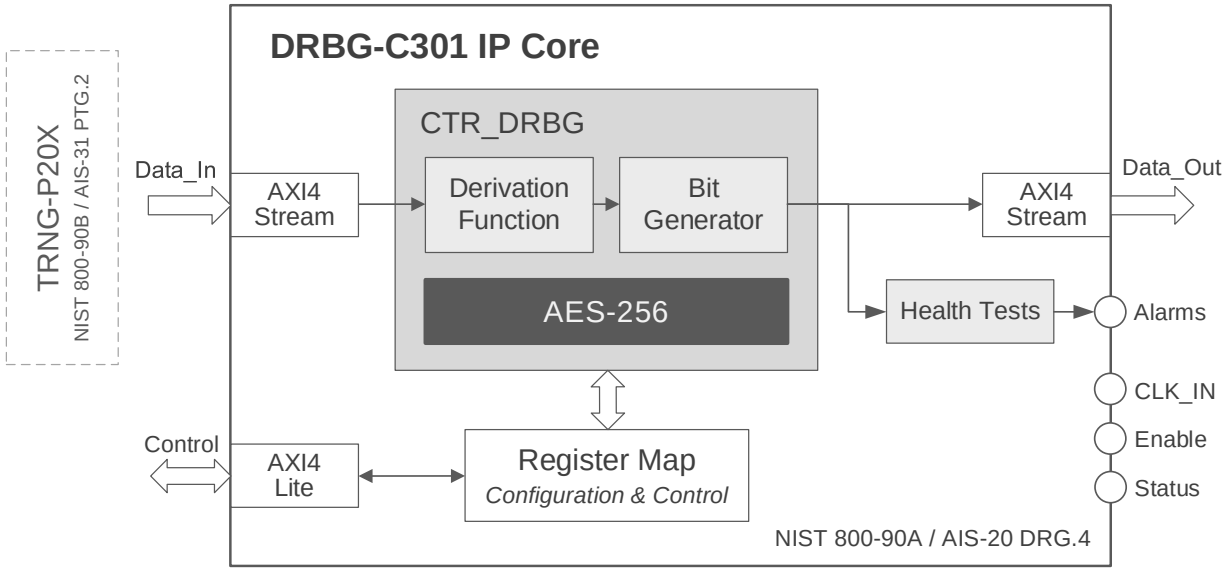
The IP core is provided as encrypted netlist for one device family, under a perpetual Site Licence. It includes 12 months of maintenance and integration support into the target platform.

Deliverables

- Targeted, timing closed Netlist
- Design Constraints
- Simulation Model
- User Manual
- ANSI C drivers

Related Products

TRNG-P20X True Randon Number Generators provide a high-quality entropy source that can be used as input seed for the DRBG-C301 IP Core.



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