ELECTRA IC
Design & Verification

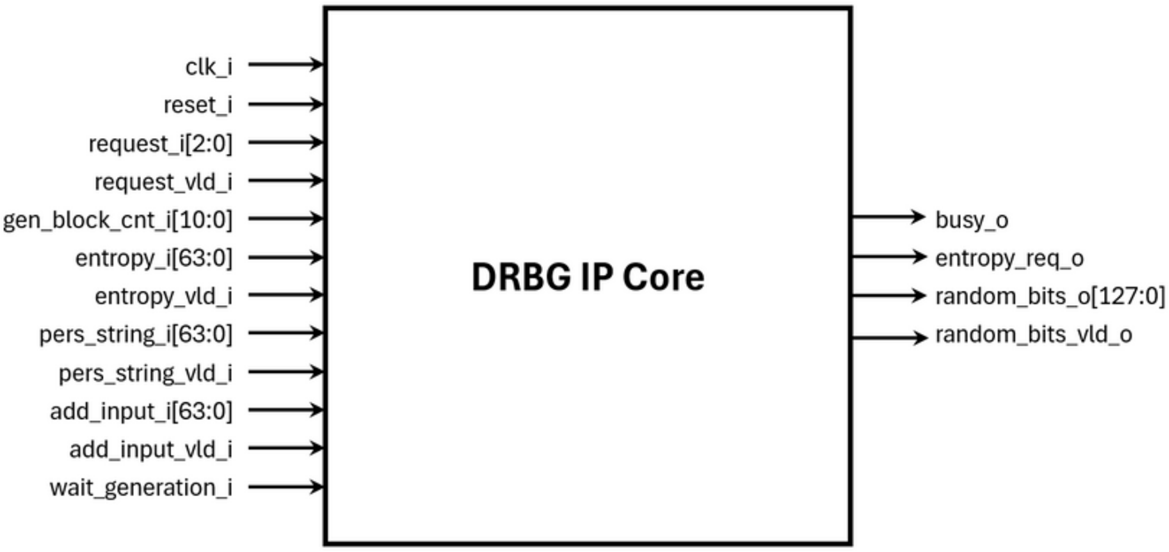
DRBG IP Core
Datasheet

November 2024

OVERVIEW

DRBG IP Cores perform deterministic random bit generation in compliance with the standards and guidelines defined in 'NIST SP 800-90A'. This standard specifies methods for generating deterministic random bits suitable for cryptographic applications.

DRBG IP Core includes the CTR-DRBG mechanism, which uses an AES-128. VHDL is used as the Hardware Description Language of the IP Core. DRBG IP Cores support various operations, including instantiation with and without personalization strings, reseeding with and without additional input, and generating random bits with or without prediction resistance and with and without additional input.



DELIVERABLES

- Encrypted Netlist
- Synthesis Scripts
- Comprehensive Documentation
- DRBG Validation System Testbenches in SystemVerilog

FEATURES LIST

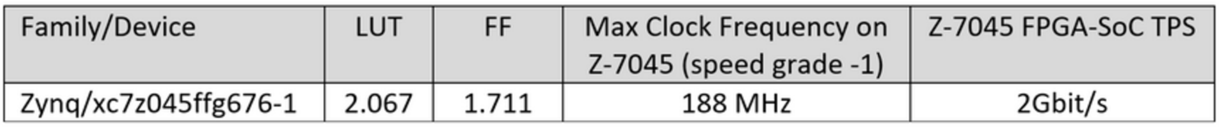
DRBG IP Core:

- is compliant with NIST SP 800-90A.
- is tested on Z-7015 Z-7020 Z-7045
- supports the operations listed below:
  - *instantiate with and without Personalization String*
  - *reseed with and without Additional Input*
  - *generate with and without Prediction Resistant and with and without Additional Input*
- has fully stallable input and output interface.

Technology Partner
prolenne DIGITAL SECURITY

FPGA SYNTHESIS RESULTS

The FPGA resources requirements



Family/Device	LUT	FF	Max Clock Frequency on Z-7045 (speed grade -1)	Z-7045 FPGA-SoC TPS
Zynq/xc7z045ffg676-1	2.067	1.711	188 MHz	2Gbit/s

LICENSING

A one-time license fee is paid with the initial IP purchase.

- Single project license
- Multi project license

MAINTENANCE & SUPPORT

- M&S fee of 15% is mandatory for the first year.
- Telephone and email support is included under M&S contract.
- IP Core updates are included in M&S.

ORDERING

- Purchase order shall include the product number EIP-9009.

Technology Partner

procenne DIGITAL SECURITY