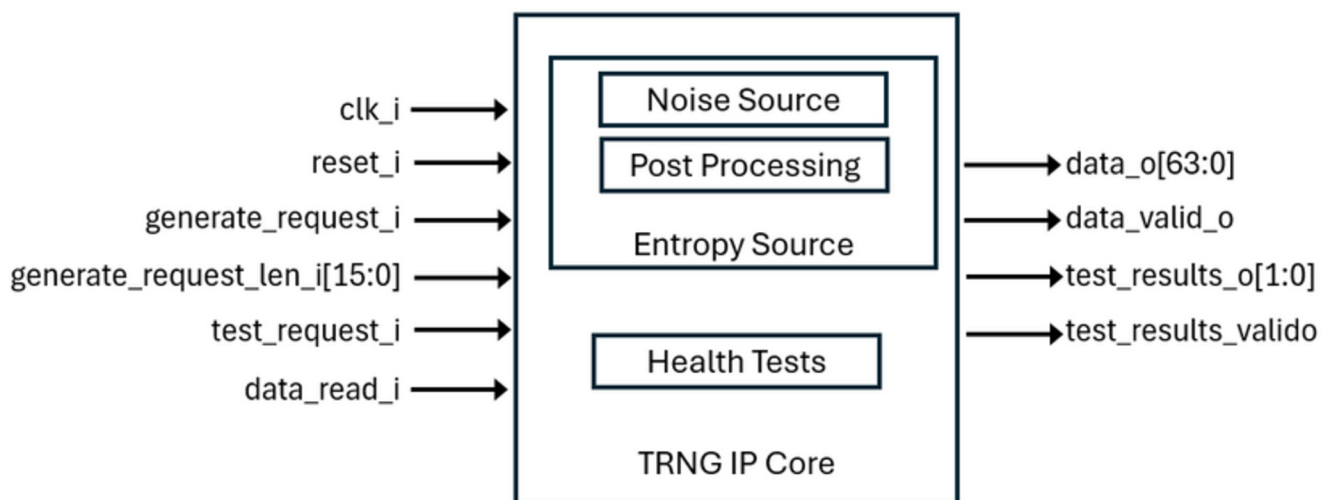


November 2024

OVERVIEW

TRNG IP Cores perform true random number generation in compliance with the standards and guidelines defined in 'NIST SP 800-90B'. This standard specifies methods for generating true random numbers suitable for cryptographic applications. TRNG IP Cores provide high-quality randomness and are designed for secure and reliable entropy generation. VHDL is used as the Hardware Description Language of the IP Core. TRNG IP Core has successfully passed the AIS-31, NIST 800-22 Statistical Test Suite, and NIST 800-90B (IID, Independent and Identically Distributed) tests.



DELIVERABLES

- Encrypted Netlist
- Synthesis Scripts
- Comprehensive Documentation

FEATURES LIST

TRNG IP Core:

- is compliant with NIST SP 800-90B.
- supports the Approved Continuous Health Tests specified in NIST 800-90B.
- supports post processing optionally.
- passes AIS-31 tests.
- passes NIST 800-22 Statistical Test Suite tests.
- passes NIST 800-90B IID tests.
- tested and approved by PCI.
- is tested on Z-7015 Z-7020 Z-7045.
- has fully stallable input and output interfaces.

Technology Partner

proLenne
DIGITAL SECURITY

TRNG IP Core

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	174	205	300 MHz	300Mbit/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-14009.

Technology Partner

