SILEX INSIGHT

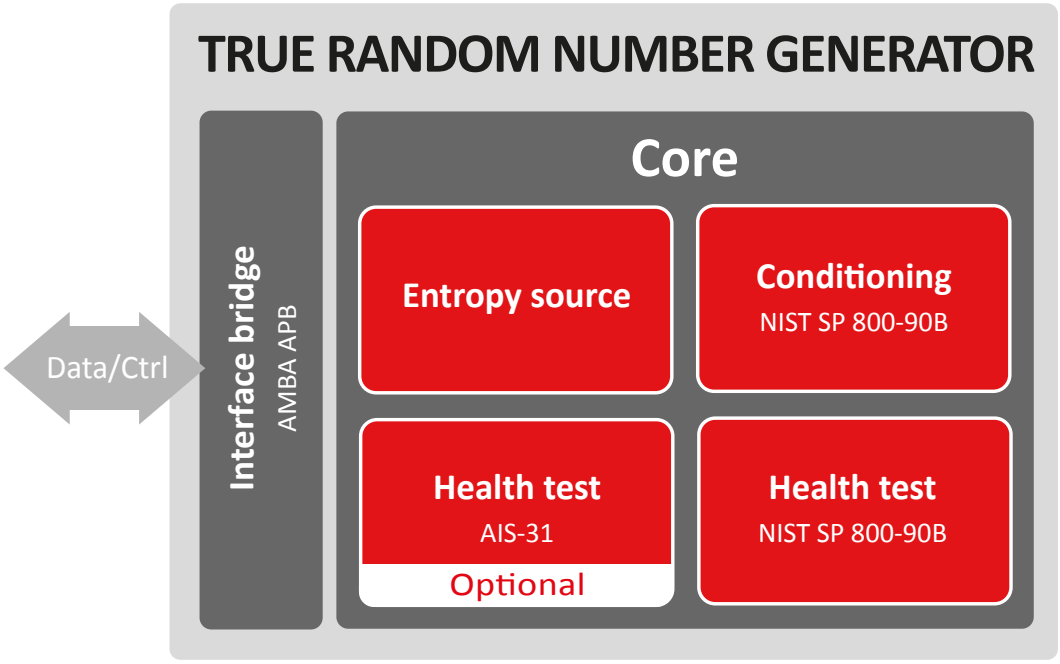
Product sheet
BA431

TRUE RANDOM NUMBER GENERATOR

The True Random Number Generator is an essential silicon-proven digital IP core for all FPGA, ASIC and SoC designs that targets cryptographically secured applications. It is a digital source of entropy designed for compliance with the NIST-800-90B and AIS31. The IP Core successfully passed NIST-800-22, 90B and AIS31 test suites on the entropy source and it is compliant with the FIPS-140-2 validation.

Random number generation is critical for any secure device. Random numbers are used for key generation, key exchange, digital signature, encryption and more. Typical secure protocols like IPsec, MACsec, TLS/SSL or wireless use them during authentication/ key exchange and data streaming phases.

The true random number generator includes conditioning function and health tests as defined in the NIST 800-90B and AIS31. Convenient AMBA APB interface is used for both control and data transfer.



Features

- NIST 800-90B compliant
- AIS-31 start-up and on-line tests (optional)
- Passed NIST 800-22, 90B and AIS31 test suites
- FIPS 140-2 compliant
- Ready for FIPS 140-3
- Portable to FPGA and ASIC technology
- Linux drivers (access from /dev/random)
- AMBA APB interface
- Pure digital

Applications

- Defense
- IPSec (VPN)
- TLS/SSL
- Automotive
- IIoT
- Wearable devices
- Embedded Security

Software Support

Linux drivers are available to ease the integration in Linux OS. The Linux driver provides direct access to the true random number generator through "/dev/random". Software driver for micro-controller application is also available to ease the control of the random generator.

Technology

The entropy source is completely digital without any specific technology-dependent implementation. It makes it easy to port it to any technology (all ASIC nodes, Intel and Xilinx FPGA families). The random generator has been used in many ASIC and FPGA designs. Products from our customers have also passed FIPS 140-2 validation.

Deliverables

- Netlist or RTL
- Scripts for synthesis & STA
- Self-checking test-bench based on FIPS vectors
- Documentation

The True Random Number Generator is available in our **Deterministic Random Bit Generator** (BA433) and **Crypto Coprocessor** (BA450).

Silex Insight
Rue Emile Francqui 11,
1435 Mont-Saint-Guibert, Belgium

Tel: +32 10 45 49 04
E-mail: contact@silexinsight.com
Web: www.silexinsight.com