XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

Pseudorandom Number Generator (PRNG)

Product codes: XIP8103B, XIP8103H

The PRNG IP core establishes a benchmark for hardware-based security in cryptographic systems by generating high-quality pseudorandom numbers. It delivers accelerated output rates essential for secure communications and cryptographic operations, such as key generation. It includes robust and thoroughly characterised initialisation and reseeding mechanisms and a proven CTR_DRBG and AES-256 based pseudorandom number generator.

The IP core conforms to the stringent NIST requirements while offering flexibility and broad compatibility for both FPGA and ASIC designs.

KEY FEATURES

- Moderate resource requirements
- High output rate - up to tens of Gbps
- Compliant with NIST SP 800-90A
- CAVP validated
- Ready for FIPS 140-3 certification
- CTR_DRBG with AES-256
- Support backtracking resistance
- Forward prediction resistance mode
- Parameterisable and fully digital design
- Easy system integration via AXI4 interface
- Vendor agnostic FPGA/ASIC implementation

APPLICATIONS

High-quality, high-output PRNG for security & performance:

- Integrate and enhance output of Quantum Random Number Generator
- Space and satellite applications
- Industrial automation solutions
- Automotive systems
- Defence

PRNG

Reliable pseudorandom numbers

BALANCED

XIP8103B

- Over 2 Gbps output
- Only ~4 .1 kLUTs in a typical FPGA setup

HIGH-SPEED

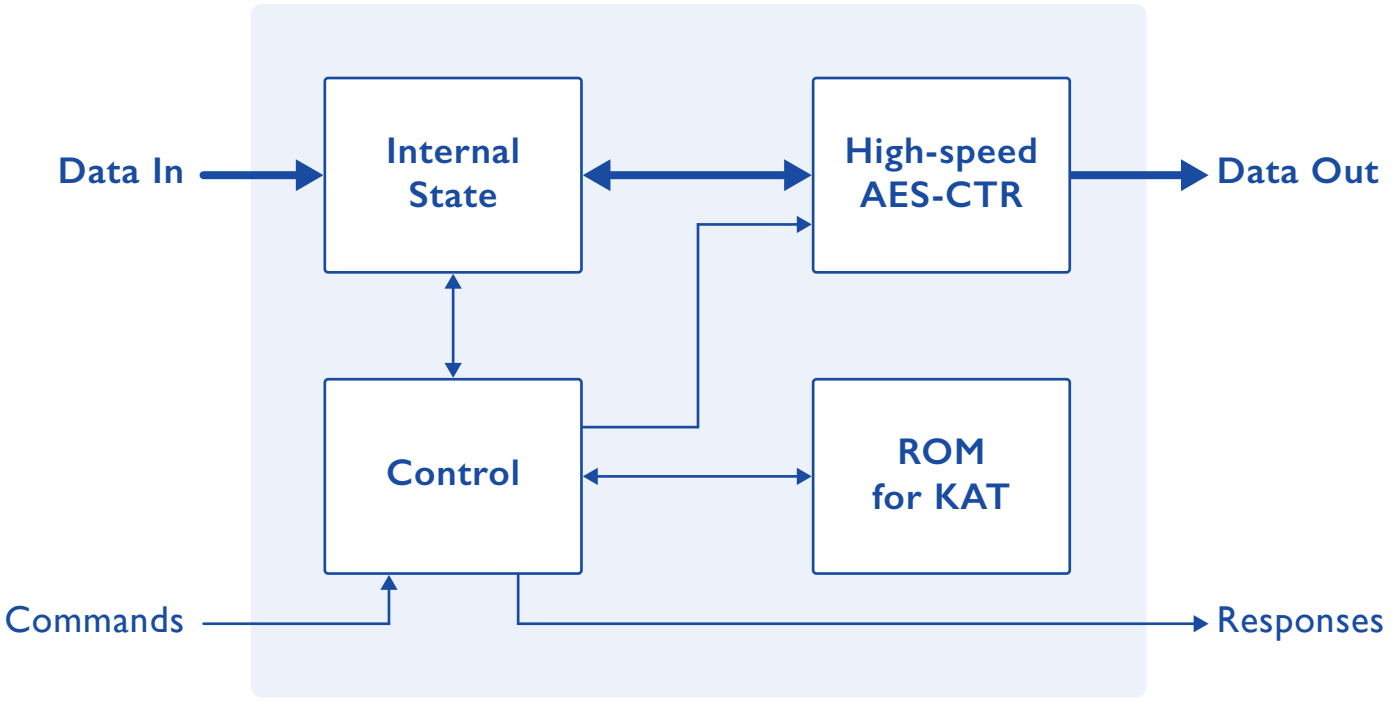
XIP8103H

- Suitable for high-throughput environments
- Over 69 Gbps output
- Only ~18 kLUTs in a typical FPGA setup

Combining the PRNG with our NIST SP800-90B compliant TRNG, provides a NIST SP800-90C compliant Random Number Generator, optimal for cryptographic security.

XIPHERA

PRNG - High-speed



Deliverables

✓ Encrypted RTL or source code	✓ Optional netlist
✓ Sample synthesis scripts	✓ Instantiation file
✓ Comprehensive simulation test bench, scripts & guide	✓ Detailed datasheet and integration guide

About Xiphera

Xiphera, Ltd, is a Finnish company designing hardware-based security solutions using standardised cryptographic algorithms. Our product portfolio consists of secure and efficient cryptographic Intellectual Property (IP) cores, designed directly for ASICs and FPGAs. Our strong cryptographic expertise, extensive experience in system design, and deep knowledge in the field of reprogrammable logic enable us to offer our customers peace of mind in a dangerous world.

XIPHERA
PEACE OF MIND IN A DANGEROUS WORLD

Tekniikantie 12
02150 Espoo
Finland

Email: sales@xiphera.com
Phone: +358 20 730 5252
Web: www.xiphera.com