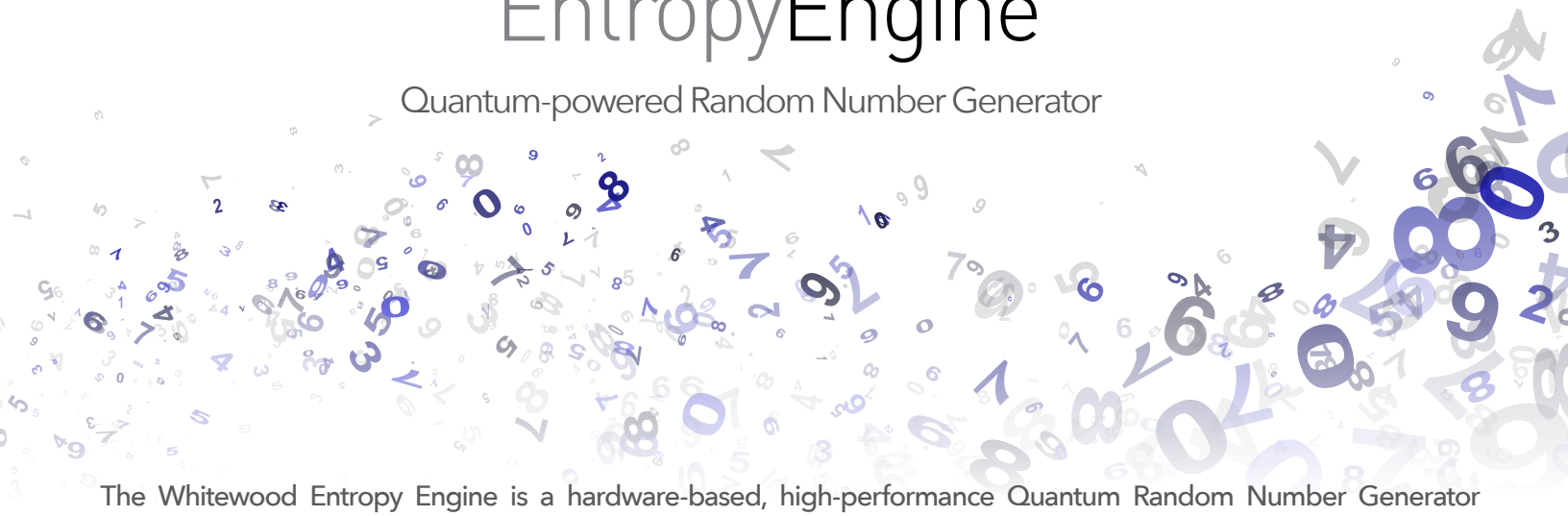
WHITEWOOD®

EntropyEngine™

Quantum-powered Random Number Generator



The Whitewood Entropy Engine is a hardware-based, high-performance Quantum Random Number Generator (QRNG) capable of generating 350 Mbit/s of true random numbers. Delivered as a standard PCI Express form factor card the Entropy Engine is a powerful plug-in module that is compatible with most server hardware variants including 1U rackmount and tower systems. The Entropy Engine is compliant with the draft NIST standard SP 800-90B, *Recommendation for the Entropy Sources Used for Random Bit Generation*.

HOW IT WORKS

The Entropy Engine incorporates our award-winning entropy source that exploits the unique properties of quantum mechanics to generate near perfect randomness. Jointly developed with Los Alamos National Laboratories the Whitewood entropy source uses the fundamentally random phenomena of light known as photon bunching to generate an exceptionally random signal that is digitized to produce a high speed stream of true random numbers. Other random number generators capture entropy from a variety of natural and man-made sources but few have the fundamental randomness and true unpredictability provided by quantum mechanics.

HOW RANDOM IS YOUR RANDOM?

It is essential to have a high level of confidence in the operation of any random number generator. Whenever an RNG's output is less than perfectly random there is an inevitable risk. But verifying randomness is notoriously difficult and attacks or failures can be undetectable. Worse still, most hardware RNGs employ cryptographic post-processing that makes them even harder to validate and test.

ENSURING CONFIDENCE

The inherently high performance and almost fully entropic source used by the Entropy Engine means it can avoid the need to perform cryptographic data processing and can provide an 'unconditioned' data output. This 'clean' output provides the direct ability to use and validate the entropy of the underlying source and to perform real-time health tests. This transparency is in contrast to most commercial and embedded RNGs that are provided as 'black box' systems with little or no ability to verify internal operation.

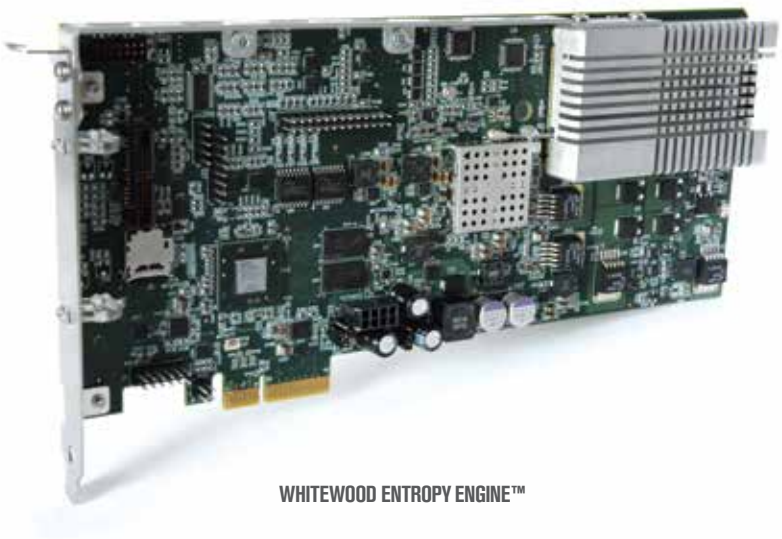
netRANDOM™

NETRANDOM – SHARE THE POWER OF GREAT ENTROPY

In addition to acting as a dedicated RNG the Entropy Engine can also be deployed as the heart of the Whitewood netRandom™ entropy management solution. netRandom is a network-based entropy distribution system for supplementing the local entropy capabilities of distributed VMs, populations of embedded systems or remote clouds to ensure all application instances have access to true random numbers.

WHITEWOOD 100 High Street 28th Floor Boston, MA 02110 USA
p. +1.617.391.0268 e. info@whitewoodsecurity.com

HARNESS THE POWER OF GREAT ENTROPY



WHITEWOOD ENTROPY ENGINE™

The Whitewood Entropy Engine has the following core capabilities:

- High performance – delivering 350Mbit/s of true random numbers
- Quantum powered entropy source – nature's source of pure randomness
- Unconditioned entropy output - enables randomness testing and validation
- Real-time self-test processes – provides confidence of correct operation
- Standard PCIe card form factor – supported by most server platforms
- Support for OS level RNGs – high performance re-seeding for existing applications
- Convenient API – simple and high-speed direct access for custom applications

Applications

- Cryptography
- Key generation
- Crypto-currency
- Tokenization
- Authentication
- Payments
- PIN generation
- Statistical research and simulations
- Gaming and lotteries

Product specification

- Entropy Source
  - Quantum: photon bunching
- Unconditioned Data Output
  - Data rate: 350 Mbit/s
  - Entropy score: >99.4% entropy
- Conditioned Data Output
  - Data rate: 200 Mbit/s
  - Entropy score: full entropy
  - Conditioning function: SHA 512
- Health Checks
  - Repetition count test (continuous)
  - Adaptive proportion test (continuous)
  - Full functional self-test (startup)
- Physical and Electrical
  - Form factor: PCIe card (3/4 length)
  - Dimensions: 236mm x 100mm x 19mm
  - Electrical interface: PCIe x4 Gen-2
  - Operating temperature: 5 to 65°C
  - Storage temperature: -25 to 85°C
  - Operating humidity: 0 to 80% RH @40°C
  - Maximum number of cards per chassis: 4
- Software and Data Interface
  - Operating system support: Linux –CentOS7 (others to follow)
  - Data exchange: PCIe 64bit DMA N-point
  - Host-side software - Linux loadable module driver and library
- Compliance and Testing
  - NIST SP 800-22
  - NIST SP 800-90B
  - Alphabit
  - Dieharder
  - FIPS 140
  - TEST U01

2016 R&D 100 WINNER

whitewoodsecurity.com

WHITEWOOD 100 High Street 28th Floor Boston, MA 02110 USA
p. +1.617.391.0268 e. info@whitewoodsecurity.com