Dragonfly

PCIe Quantum Random Number Generator

High Performance. Low Power. Quantum source Entropy.

Crypta Labs introduces Dragonfly – the fastest PCIe Quantum Random Number Generator (QRNG) device used to provide the highest quality source of entropy possible.

Our fastest ever PCIe QRNG

Dragonfly outputs Quantum Random Numbers at a **rate of 300Mbps** and is compatible with hosts running Linux based Operating systems, making it perfect for deployment in server based or rack mounted hosts requiring **next level performance**.

Cutting edge QRNG Technology

Crypta Labs Quantum Optics Module (QOM) utilises a light source and photon detector which is calibrated to measure quantum noise. This raw noise is then passed through our **QEngine technology,** which performs Real-time Health Tests and Post Processing functions which were designed from the ground up to limit performance loss from point of photon capture to delivery of a random number. **Our output has been independently verified to pass tests from both NIST as well as the demanding TESTU01 suites.**

| **Quantum Powered** Equipped with our Quantum Optics Module	**Robust & Reliable** NIST Compliant output in real world environments	**High performance** Our fastest QRNG yet, ideal for servers	**Easily Adoptable** Low profile PCIe card measures only 7cmx7cm

Tomorrows technology for a safer today

Current Pseudorandom (PRNG) and hardware True (TRNG) number generation technologies have intrinsic vulnerabilities. PRNG's can be subject to algorithmic attacks. TRNGs have throughput speed limitations, especially in different environmental conditions, which leave a question mark over their suitability for deployment in demanding networks and operations requiring the highest levels of entropy.

Our QRNG technology is robust in any environment and contains health monitoring and in-the-field calibration techniques to ensure output quality is never compromised.
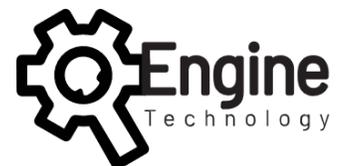
QRNG

Health Monitoring

NIST Compliant

Market leading adoptability

With a specification which meets the needs for the future of connected devices and IoT, our QRNG is deployed via a PCIe interface – making retrofitting to your host a breeze!

Our Quantum Optics Module (QOM) technology, coupled with onboard processing capabilities in an easily integratable package to produce a usable random output which betters our competitors in both quality and robustness.

Why Choose Crypta Labs?

- Best quality RNG output in the market - proven by independent testing Universities
- Designed and built for tomorrows threats
- Designed for use in the real world
- Tamper protection and health monitoring at the core
- Configurable in clusters for greater performance
- Built in line with NIST standards

Device Specification

Model	Dragonfly QRNG
Performance	300Mbps (~1,171,800 Random Numbers per second*)
NIST Compliant output	Yes (not yet certified)
QRNG Quality Independently verified	Yes
OS Support	Linux Source Drivers. In kernel compile possible.
Entropy Source	1 x Quantum Optics Module
Size	7cm x 7cm
Power	
Single Input Voltage	3.3V
Normal operation draw	2W
Startup from Idle	<1ms
Recommended operating Temperature	-30°C ~ +85°C
Max operating Temperature	-40°C ~ +125°C
Interface	
PCIe	Gen2 x1

*Assumes random number of 256bits

The information in this sheet is subject to change and is for illustrative purposes only