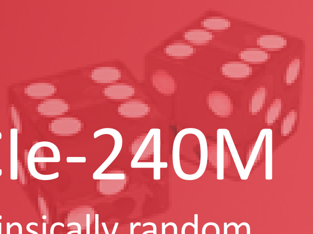
Redefining Randomness

Quantis QRNG PCIe-40M & PCIe-240M



Only Quantum Random Number Generators (QRNGs) are intrinsically random and provably unpredictable

Since 2001, the Quantis QRNG family is commonly used as trusted source of randomness for multiple applications: to generate high-quality keys needed by cryptographic modules, to effectively protect access to private networks, servers, virtual machines and applications; to protect data integrity and confidentiality. Other applications include gaming, scientific simulations or modeling.

Provably secure

Simplicity is the strength of the ID Quantique Quantum Random Number Generators (QRNGs). The Quantis QRNG family exploits elementary quantum optic processes that are fundamentally probabilistic to produce true randomness. As the quantum processes underlying the QRNG are well understood and characterized, their inner working can be clearly modelized and controlled to produce the highest entropy from the first bit.

Quantis PCIe-40M and PCIe-240M embed IDQ20MC1 chips, ID Quantique's latest QRNG technology, that generate randomness from the shot noise of a light source captured by a CMOS image sensor. They can generate random bits directly from the entropy source (entropy data mode), or after a NIST compliant post-processing (RNG data mode). Live status verification and entropy source health monitoring performed at chip level ensure the PCie cards always provide the highest entropy, and any failure or attacks are detected.

Compliant and certified

The new Quantis PCIe-40M and PCIe-240M are compliant with NIST SP800 90A/B/C recommendations and passes IID, non-IID tests, DieHarder and NIST SP800-22 test suites. METAS and CC certifications of these two new products are under way.

Legacy Quantis PCIe and USB have been certified by leading commercial entities, well-known international institutes and governments worldwide. Legacy PCIe and USB also present an AIS31 version that is compliant with the German BSI's AIS31 validation criterias.

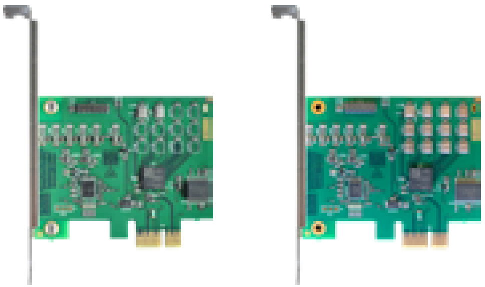
Applications

- Confidentiality and integrity of sensitive data
- Artificial Intelligence (Machine and Deep Learning)
- Security of end-consumer devices, machines and networks
- Scientific Modeling & Simulations
- Financial transactions / Blockchain
- Gaming / Random drawings

Quantis QRNG modules

Why choose Quantis QRNGs?

- Provably secure source of entropy
- True randomness from the first bit
- Quantum optical process, intrinsically random
- Integrated NIST compliant post-processing
- Live status verification & entropy source health monitoring
- Easy Integration in most operating systems



Quantis QRNG modules at a glance

Model	PCIe-40M	PCIe-240M
PERFORMANCE		
Quantum entropy source	38.3 Mbps ± 5%	232 Mbps ± 5%
RNG Data Output (embedded NIST compliant DRBG)	9.6 Mbps ± 5%	58 Mbps ± 5%
Live status verification & entropy source health monitoring	✓	✓
CERTIFICATIONS		
NIST SP800-90A/B/C, SP800-22 and DieHarder test suite compliance	✓	✓
BSI Common Criteria & AIS 31 certification	pending	pending
ENVIRONMENTAL		
Thermal noise contribution	<1% (fraction of random bits arising from thermal noise)	
Storage temperature	-40 °C to +85 °C	-40 °C to +85 °C
Operating temperature	0 °C to +50 °C	0 °C to +50 °C
PHYSICAL CHARACTERISTICS		
Dimensions (mm)	80 x 63.75	80 x 63.75
Specification	PCI Express Base 1.0a compliant	
OS SUPPORTED (QUANTIS LIBRARY AND EASYQUANTIS APPLICATION)*		
Windows 10	✓	✓
Ubuntu 18.04	✓	✓
CentOS 7	✓	✓

(*) Quantis library enables the production of random binary data, integers and floating point numbers. It can be used to access multiple Quantis generators and includes advanced functionalities such as random data scaling. The Quantis extensions libraries implement a randomness extractor which can be used to postprocess the output of the Quantis QRNG. Easy Quantis application allow to read and display random numbers or store them in a file.

Disclaimer: The information and specification set forth in this document are subject to change at any time by ID Quantique without prior notice.