THE
QUANTUM WORLD
CORPORATION

P.O. Box 51330, Albuquerque, NM 87181
(505) 222-0612 • contact@ComScire.com

February 1, 2018

To Whom it May Concern,

ComScire® – Quantum World Corporation guarantees that its QNG Model PQ32MS *Pure Quantum*™ hardware true random number generator will pass any properly designed test for randomness. Furthermore, the PQ32MS's design makes it virtually impervious to any attempt to influence or control the random output sequence.

Every true random number generator (TRNG) requires a physical source of entropy. Entropy is in general a measure of disorder in a physical system. In terms of Information Theory, entropy can be thought of as a measure of how unpredictable the measured properties of the entropy source are. Quantum entropy may be sampled to produce what is considered the most fundamentally unpredictable random numbers possible. The quantum entropy source in the QNG Model PQ32MS is shot noise due to sub-threshold leakage and gate tunneling leakage in MOS transistors. In addition, sources of chaotic entropy include a combination of thermal or Johnson noise, other types of transistor noise and switching noise. Ninety-six independent, high frequency oscillating signal sources, each producing a predetermined amount of quantum entropy and chaotic entropy, continuously operate at different frequencies between 200 and 400 MHz. Each oscillator is sampled at multiple taps to produce enhanced outputs and the enhanced outputs are further combined to produce noisy output signals. Three hundred and fifteen of these noisy signals are combined to produce a single sampled binary signal at 128 Mbps.

The PQ32MS contains three independent generators of the type described above. The statistics of each of these three generators is continuously monitored in the generator hardware. The monitoring includes 1/0 bias, 1^{st} order autocorrelation and an estimated minimum entropy. The outputs of the three generators are combined to produce one data stream at 128 Mbps, and finally blocks of 4 non-overlapping consecutive bits are XORed together to produce each final output bit at 32 Mbps. The internal hardware monitoring requires at least two of the three generators to have an estimated entropy of at least 0.999 bits/bit. If this requirement fails, the output from the generator is automatically halted. Output bits are also tested for entropy, and the generator will be halted if the output estimated entropy falls below 0.999 bits/bit. The internal hardware testing also acts as a startup test program. At startup random data will not be output until a block of 1,048,576 bits (2^{20} bits) from at least two of the three redundant generators has produced the required minimum estimated entropy level.

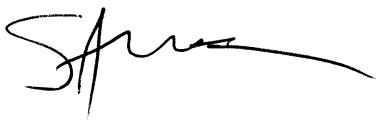
Quantum entropy of each output bit is estimated at 0.99+ bits per bit. Total entropy is indistinguishable from 1.0 and far surpasses the NIST recommendation for *full entropy* without any randomness correction or conditioning required.

Interface software in the host computer monitors the flow of data from the generator. If the monitoring program detects a halt condition, a request for the internal statistics from the raw data streams will be automatically generated. These statistics are checked to determine if there has been an actual fault in the hardware, and if this check indicates a fault, an error message will be generated and no random data will be provided. The automatic check of the hardware may also indicate there was simply a delay caused by normal functioning in the computer's operating system, programs or other attached components. If the check shows the hardware is operating correctly, the monitoring software will restart the generator output and random data flow will resume. The internal statistical test results are accessible at any time through simple commands in the user interface.

The generator is housed in a grounded, 1/16 inch aluminum device enclosure, which prevents both monitoring of output bits and interference with the generator by electromagnetic fields. Power is provided through the USB connector and is filtered at entry into the shielded enclosure. Independent regulation of power for the generator section prevents any external effect on the random number generation by fluctuations in the power source. The generator may be placed inside a computer enclosure and connected by internal USB if additional physical security is required.

The PQ32MS is used for cryptographic purposes as well as online gaming and other applications requiring the highest levels of security and randomness properties. The PQ32MS has been tested extensively using well-known test suites such as DIEHARD and NIST 800-22. In addition, each generator is continuously tested by our QNGmeter test suite to 1 trillion bits or more to verify compliance with our internal specifications, which are more stringent than either DIEHARD or NIST testing.

Sincerely,



Scott Wilber, President