The Quantum World Corporation – ComScire
P.O. Box 51330, Albuquerque, NM 87181-1330
(505) 222-0612 • contact@comscire.com
https://comscire.com

December 10, 2019

To Whom It May Concern,

ComScire® – Quantum World Corporation guarantees that its cryptographically strong hardware true random number generator, *CryptoStrong*™ Model CS128M, will pass any properly designed test for randomness. The next bit in any sequence of output bits will not be predictable beyond chance by any present or future computational means, including arbitrarily advanced quantum computers. The CS128M'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. The entropy source in the Model CS128M is quantum mechanical due to shot noise from sub-threshold leakage and gate tunneling leakage in MOS transistors, and chaotic, including a combination of thermal or Johnson noise, shot noise, other types of transistor noise and switching noise. Forty-eight independent, high frequency ring oscillator signal sources, each producing a predetermined amount of physical entropy, continuously operate at different frequencies between 200 and 400 MHz. Each oscillator is sampled at multiple signal taps to produce enhanced outputs and the enhanced outputs are further combined to produce noisy output signals. Four hundred and eighty of these noisy signals are combined to produce a single sampled binary signal at 128 Mbps.

The CS128M contains three independent entropy sources 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, 1st order autocorrelation and estimated minimum entropy. The outputs of the three entropy sources are combined to produce one final output stream at 128 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 from the entropy source is 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 used to produce a generator 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.

Total entropy from the entropy source is indistinguishable from 1.0 and far surpasses the NIST recommendation for *full entropy* without any randomness correction or conditioning. Statistical defects in the final output of the entropy source are immeasurably small.

The Model CS128M is both NIST SP 800-90C and BSI AIS 20/31 Class PTG.3 compliant. Compliance is accomplished by including an approved cryptographic post-processing deterministic random bit generator (DRBG), which accesses the full entropy required from an approved entropy source such as the one described above. The post-processing DRBG mechanism is the NIST-approved block cipher in counter mode, CTR_DRBG, using the cryptographic primitive AES with security strength of 256 bits (AES-256). The DRBG is instantiated with random input from the entropy source prior to output generation. Periodic reseeding of the internal states with fresh entropy – more than 15 times a second – is implemented to offer additional defense against attacks and for hardening the RNG design. Known-answer test (KAT) is implemented within the DRBG mechanism boundary. Testing is conducted on each DRBG function prior to the first use (at boot-up after initial entropy health test is passed) and immediately prior to each reseeding of the internal states.

Finally, the DRBG output is exclusive-ORed (XORed) with fresh entropy for every output of the TRNG at a rate of 128 Mbps. This method offers the highest possible level of reliability and protection against attacks.

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. 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 offline 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. Additional design security features were added to the Model CS128M to protect the hardware against unauthorized copying, reverse engineering, and tampering of configuration files. The firmware configuration bitstream is encrypted with AES-256 and Tamper Protection Mode is enabled. Tamper Protection Mode prevents the firmware from being read or modified by burning a fuse within the device – an irreversible process. USB interface generator-specific information is write-protected after manufacture. The generator may be placed inside a computer enclosure and connected by internal USB if additional physical security is required.

The CS128M is used for cryptographic purposes as well as online gaming and other applications requiring the highest possible levels of security and randomness properties. The CS128M 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 10 trillion bits or more to verify compliance with our internal specifications, which are more stringent than either DIEHARD or NIST testing.

The random generation method used in the CS128M is highly resistant to failure due to long-term aging, and is tolerant to expected process variations, operating temperature and supply voltage levels. The high level of redundancy provided by the three independent entropy sources and the large number of entropic bits used to produce each output bit ensures consistent and highest quality true random numbers for any application.

Sincerely,

Scott A. Wilber, President
The Quantum World Corporation