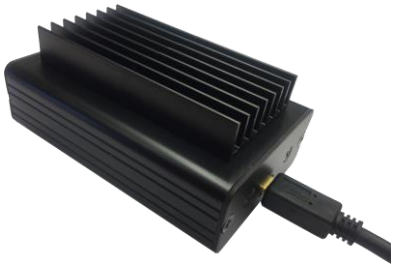
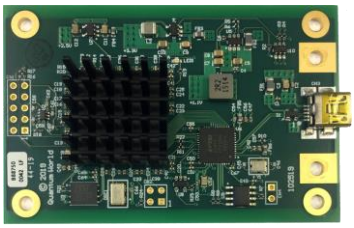
ComScire®
Quantum Number Generators

Data Sheet – ComScire® QNG Model CS128M





Features

- Designed for compliance with NIST SP 800-90C and BSI AIS 20/31 Class PTG.3 Standards
- Cryptographic post-processing: AES cipher with security strength of 256-bits (AES-256)
- Continuous hardware runtime testing with automatic halt
- Raw data stream and internal statistics available
- Independent power regulation for generator circuitry
- Encrypted firmware with tamper-protection
- USB generator-specific data write-protected
- Includes drivers, interface and testing software

Applications

- For applications requiring the highest security and fastest generation rate of guaranteed unpredictable true random numbers
- Military/Space Communication Systems
- Electronic Financial Transactions
- Cryptography
- Data Security
- Research
- Games of Chance

Specifications

- 128 Megabit per second ± 0.1%
- Statistical defects < 10^{-100}
- Estimated total entropy: $(1 - \varepsilon)$ bits per bit, $\varepsilon < 10^{-200}$
- Shielded 1/16-inch aluminum enclosure
- USB 2.0 High-Speed interface
- Bus Powered: 325mA max at 5V from USB connection. High current USB port or powered hub recommended
- Non-condensing humidity
- Operating temperature: 0-50 Deg. C
- Dimensions (L x W x H): 80 x 54 x 35 mm

System Requirements

- 32/64-bit Windows 7/2012/8/10/2016
- Linux
- USB 2.0 High-Speed host/hub

Notes:

- Minimum OS required is Windows 7 or Linux 2.6

White Paper

- The ComScire® CryptoStrong™ Random Number Generator.

Designed to meet NIST SP 800-90C and BSI AIS 20/31 Recommendations

NIST DRAFT Special Publication 800-90C, Recommendation for Random Bit Generator (RBG) Constructions, specifies the construction of approved RBGs using the DRBG mechanisms and entropy sources from SP 800-90A and SP 800-90B. The German BSI AIS 20/31 Standards proposes a methodology of constructing and evaluating random number generators (RNG). ComScire *CryptoStrong*™ Model CS128M is designed to be fully compliant with these recommendations.

GUARANTEED to Pass ANY Test for Randomness!

ComScire *CryptoStrong*™ random generators are guaranteed to pass any properly designed test for randomness. All Model CS128M generators are tested to at least 10 terabits at the time of manufacture as part of our QA program. Our testing procedures are more stringent than any other manufacturers'.

Start-Up and Runtime Testing & Cryptographic Post-Processing

CS128M includes start-up and runtime internal hardware testing of the redundant raw entropy sources and the cryptographic post-processing to ensure completely unpredictable random numbers are always being supplied to your application. The output is immediately disabled and an error message sent if any internal test fails.

For more information on any of our products or services please visit us on the Web at: https://comscire.com

P.O. Box 51330, Albuquerque, NM 87181 • Phone 505.222.0612

Made in USA RoHS Compliant