ComScire QNG Model CS128M
Validation Tests of Randomness

Table of Contents

ComScire QNGmeter: Continuous Random Number Tester.

The ComScire QNGmeter is a continuous real-time statistical tester that uses five powerful and fundamentally different tests on the input data. Unlike other statistical test suites, it is designed to measure the quality of randomness of a continuous sequence of bits up to hundreds of terabits in length. The QNGmeter automatically performs metatests of subsequences, which would have to be done manually by other popular test suites. Every QNG Model CS128M is tested extensively after production and finally just before shipment using the QNGmeter test suite.

The five tests are:

1) 1/0 Balance – nominal expected value is $p(1) = p(0) = 0.5$.
2) Auto Correlation - orders 1 through 32, nominal expected value is 0.5 for all orders.
3) Entropy Test – nominal expected value is H = 1.0, an update of U. Maurer's "Universal Test" [Cor99].
4) Serial Test - (Good, I. J, The serial test for sampling numbers and other tests for randomness, *Proc. Camb. Philos. Soc.* Vol. 49, 1953).
5) OQSO – Overlapping-Quadruples-Sparse-Occupancy test, nominal expected value for the mean = 141909.47 and standard deviation (by simulation) = 294.656 (G. Marsaglia and A. Zaman, *Computers Math. Applic.*, Vol. 26, No. 9, pp 1-10, 1993).

The z-scores, p-values, and chi-square (metatest) p-values are presented for each test. In addition, current test run time information, such as *Bits Tested*, *Elapsed Time*, *Throughput*, and *Bits Tested %,* is displayed by the tester. *Bits Tested* is the total number of bits tested. *Elapsed Time* is the time from the start of the current test run. *Throughput* is the input data rate in bits per second. *Bits Tested %* is the percent of the total bits tested. This value might be less than 100% due to limited CPU resources.

Each test uses blocks of data of varying lengths, depending on the specific test. The 1/0 Balance and Auto Correlation tests use a block size of 65,536 bits. The Serial test has a block size of 262,144 bits. The Entropy test has 4,194,304 bits in a block. The OQSO test uses 10,485,775 bits per block.

A z-score is calculated for every test for each data-block. The z-scores are converted to probabilities with the assumption they are normally distributed. The z-scores of the 1/0 Balance, Auto Correlation and Serial tests and their associated p-values displayed are cumulative for all blocks. The z-scores of the Entropy and OQSO tests are combined by summing the z-scores of all blocks and dividing by the square root of the number of blocks, respectively.

A second level of testing is applied to the p-values calculated from the z-scores for each block of data. The z-scores are expected to be normally distributed and their associated p-values are expected to be uniformly distributed. A chi-square test is applied to the individual p-values from each of the five tests. The chi-square tests are cumulative and their results are displayed as probabilities. If these chi-square p-values converge to 0.0 or 1.0 for any test, the assumption of randomness fails, indicating non-random patterns in the data being tested.

A third level of testing is applied to all of the individual chi-squared tests. A Kolmogorov-Smirnov (KS) test is first applied to the probabilities of chi-squared results of all orders of auto correlation being tested to reduce the auto correlation results to a single probability. A meta-meta

KS test is finally calculated using the auto correlation KS result and the probabilities of the chi-squared metatest results of all the other tests. The meta-meta KS+ and KS- probabilities are displayed. Convergence toward 1.0 or 0.0 indicates failure.

For the hardware validation report, the QNGmeter tests were completed on a QNG Model CS128M using 710 trillion random bits. All metatest results for the device are recorded in the following Table 1.

ComScire QNGmeter 710 Trillion Bits Tested **Testing QNG Device S/N QWR80001**			
Run Time Information		**Autocorrelation**	
Bits Tested	**710E+12**	**Order**	**p ($\chi^2 \le x$)**
Time Elapsed	**153:05:26:23**	**1**	**0.411814**
Throughput	**128E+6**	**2**	**0.069432**
Meter	**47.3+**	**3**	**0.121966**
1/0 Balance		**4**	**0.113409**
p (1)	**0.5000000038**	**5**	**0.205724**
p ($z \le x$)	**0.578920**	**6**	**0.449533**
p ($\chi2 \le x$)	**0.965719**	**7**	**0.651279**
Entropy Test		**8**	**0.466550**
H	**1.0000000216**	**9**	**0.312043**
p ($z \le x$)	**0.922749**	**10**	**0.432477**
p ($\chi^2 \le x$)	**0.109109**	**11**	**0.315501**
Serial Test		**12**	**0.362202**
p ($z \le x$)	**0.709419**	**13**	**0.042787**
p ($\chi^2 \le x$)	**0.091264**	**14**	**0.313442**
OQSO (Monkey Test)		**15**	**0.310035**
p ($z \le x$)	**0.067075**	**16**	**0.636126**
p ($\chi^2 \le x$)	**0.366756**	**17**	**0.936125**
AC Meta KS- Test		**18**	**0.634828**
KS-	**0.277938**	**19**	**0.081837**
Meta-Meta KS Test		**20**	**0.285263**
KS+	**0.885590**	**21**	**0.422316**
KS-	**0.306019**	**22**	**0.733124**
		23	**0.879618**
		24	**0.697534**
		25	**0.996296**
		26	**0.539955**
		27	**0.336305**
		28	**0.245446**
		29	**0.528274**
		30	**0.637863**
		31	**0.861949**
		32	**0.836153**

Table 1 — QNGmeter continuous test results for CS128M.

NIST Statistical Test Suite for the Validation of Random Number Generators.

The National Institute of Standards and Technology (NIST) provides a statistical testing suite, specified in Special Publication 800-22rev1a, consisting of 15 tests that were developed to test the randomness of binary sequences generated by a TRNG or PRNG. The NIST Statistical Test Suite (NIST STS) software and documentation can be downloaded from their Cryptographic Toolkit web page.

The NIST STS source code was compiled on a computer running Ubuntu 18.04. A number of tests were completed to confirm the functionality of the software. The test suite contains sample data files of 1,000,000 bits in length to be analyzed. These include the binary expansions of constants *e*, π, √2 and √3. For each sample file, the NIST STS battery of tests were performed and compared to the empirical results found in the SP800-22rev1a documentation Appendix B. Following the confirmation that the test suite is operating properly, a binary file of 1 billion raw random bits in length was generated using our QNG Model CS128M (SN: QWR80001) to be analyzed.

All test results are recorded in the following Table 2. The Block Frequency, Non-overlapping Template Matching, Overlapping Template Matching, Approximate Entropy, Linear Complexity and Serial tests require user prescribed input parameters. The exact values used in these examples have been included in parenthesis beside the name of the statistical test. In the case of the Non-overlapping Templates test, a Kolmogorov-Smirnov test (KS-test) was performed for the collection of 148 *P-values*. In the case of the Random Excursions and Random Excursions Variant tests, KS-tests for the collection of 8 and 18 *P-values*, respectively, have been reported.

NIST Battery of Tests Results	
Statistical Test	**P-value**
Frequency	0.630872
Block Frequency (m = 128)	0.781106
Cumulative Sums-Forward	0.809249
Cumulative Sums-Reverse	0.268917
Runs	0.137282
Long Runs of Ones	0.058243
Rank	0.666245
Spectral DFT	0.074791
Non-overlapping Templates (m = 9)	0.138219
Overlapping Templates (m = 9)	0.408275
Universal	0.200115
Approximate Entropy (m = 10)	0.878618
Random Excursions	0.892380
Random Excursions Variant	0.133669
Linear Complexity (m = 500)	0.570792
Serial (m = 16, $\nabla\Psi^2{}_m$)	0.188601
Serial (m = 16, $\nabla^2\Psi^2{}_m$)	0.122325

Table 2 — NIST Test Suite Results for CS128M.

NIST SP 800-90B Entropy Source Validation.

NIST Special Publication (SP) 800-90B provides a standardized process of validating the entropy source quality. The process includes the following steps:

1) Data Collection
2) Determine the track (IID or Non-IID)
3) Initial Entropy Estimate
4) Restart Tests
5) Update Entropy Estimate
6) Entropy Validation

NIST offers software for the initial entropy estimation, restart tests and update entropy estimation. The source code and documentation is available from NIST GitHub repository[1]. The source code was compiled on a computer running Ubuntu 18.04. The included self-test was performed to confirm the functionality of the software.

1. Data Collection.

A sequential dataset of at least 1,000,000 samples must be obtained directly from the noise source to determine the initial entropy estimate. If the generation of 1,000,000 consecutive samples is not possible, the concatenation of several smaller sets of consecutive samples from the same source is allowed. Smaller sets shall contain at least 1,000 samples.

For the restart tests, the entropy source must be restarted 1,000 times; for each restart, 1,000 samples shall be collected.

2. Determine Entropy Track.

Entropy estimation is completed based on selecting from two different tracks: IID and non-IID. The IID-track applies for entropy sources that provide IID (independent and identically distributed) numbers, whereas the non-IID track applies for entropy sources that do not provide IID numbers.

The CS128M entropy source provides IID numbers (see CryptoStrong White Paper).

3. Initial Entropy Estimate.

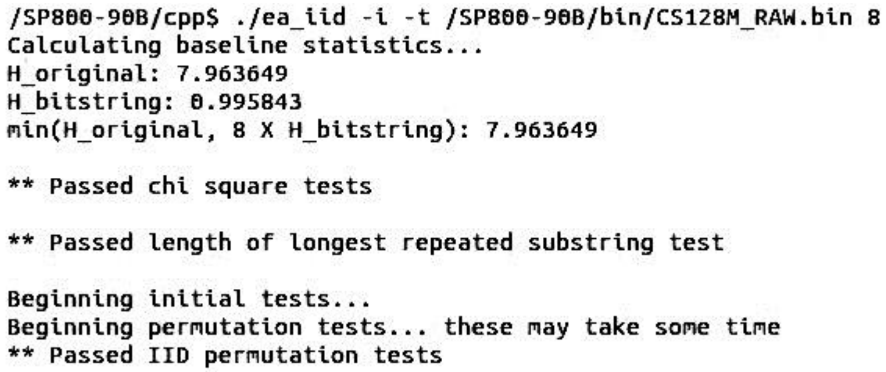
The submitter shall provide an entropy estimate, denoted as $H_{submitter}$, for the noise source outputs, which is based on the submitter's analysis of the noise source. See CryptoStrong White Paper for in-depth submitter entropy estimation. After determining the entropy estimation track, a min-entropy estimate of the collected sequential dataset of 1,000,000 samples, denoted as $H_{original}$, is calculated using the NIST software. Then, the initial entropy estimate is determined as $H_I = \min(H_{original}, H_{submitter})$. Submitter entropy estimate, NIST initial entropy estimate, the initial

[1] https://github.com/usnistgov/SP800-90B_EntropyAssessment

min-entropy estimate, and additional statistical tests results are reported in Table 3. Figure 1 is a screenshot of the actual test run.

NIST SP 800-90B Entropy Assessment	
Initial Entropy Estimate	
Statistical Test	**Results**
$H_{submitter}$	8.000000
$H_{original}$	7.963649
H_I = min ($H_{original}$, $H_{submitter}$)	7.963649
Chi Square Tests	PASS
Length of Longest Repeated Substring Test	PASS
IID Permutation Tests	PASS

Table 3 — NIST Initial Entropy Estimate for CS128M.



```
/SP800-90B/cpp$ ./ea_iid -i -t /SP800-90B/bin/CS128M_RAW.bin 8
Calculating baseline statistics...
H_original: 7.963649
H_bitstring: 0.995843
min(H_original, 8 X H_bitstring): 7.963649

** Passed chi square tests

** Passed length of longest repeated substring test

Beginning initial tests...
Beginning permutation tests... these may take some time
** Passed IID permutation tests
```

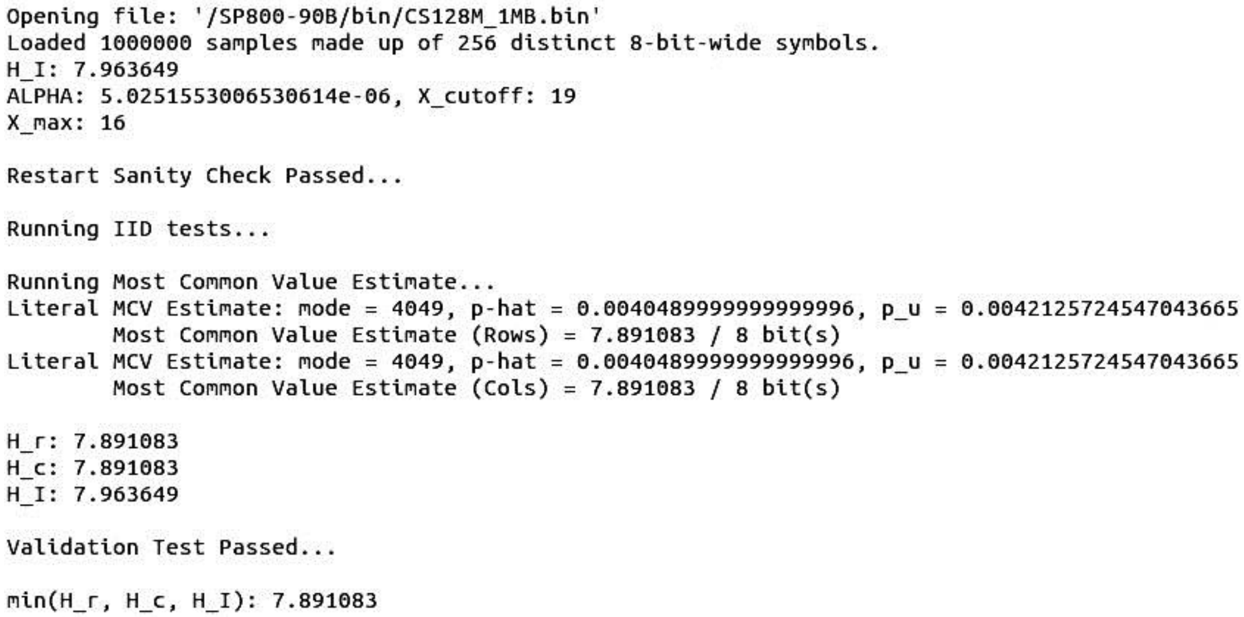
Figure 1: NIST IID-Track Initial Entropy Estimate Test for CS128M

4. Entropy Validation: Restart Tests and Update Entropy Estimate

The restart tests re-evaluate the entropy estimation for the noise source using different outputs from many restarts of the noise source. A matrix *M* of row *r* =1,000 and column *c* = 1,000 is constructed from the collection of restart samples. Sanity check is performed on the matrix *M* prior to calculating entropy estimates on the row and column datasets. The entropy estimates from the row (H_r) and the column (H_c) datasets are expected to be close to the initial entropy estimate H_I. If the minimum of H_r and H_c is less than half of H_I, the validation fails, and no entropy estimate is awarded. Otherwise, the entropy assessment of the noise source is taken as the minimum of the row, the column and the initial estimates, i.e., min (H_r, H_c, H_I). The results are presented in Table 4. Figure 2 is a screenshot of the actual test run.

NIST SP 800-90B Entropy Assessment	
Restart Tests and Update Entropy Estimate	
Statistical Test	**Results**
H_I	7.963649
H_r	7.891083
H_c	7.891083
min (H_r, H_c, H_I)	7.891083
Restart Sanity Check	PASS
Entropy Validation Test	PASS

Table 4 — NIST Validation at Entropy Estimate for CS128M.



```
Opening file: '/SP800-90B/bin/CS128M_1MB.bin'
Loaded 1000000 samples made up of 256 distinct 8-bit-wide symbols.
H_I: 7.963649
ALPHA: 5.0251553006530614e-06, X_cutoff: 19
X_max: 16

Restart Sanity Check Passed...

Running IID tests...

Running Most Common Value Estimate...
Literal MCV Estimate: mode = 4049, p-hat = 0.0040489999999999996, p_u = 0.0042125724547043665
        Most Common Value Estimate (Rows) = 7.891083 / 8 bit(s)
Literal MCV Estimate: mode = 4049, p-hat = 0.0040489999999999996, p_u = 0.0042125724547043665
        Most Common Value Estimate (Cols) = 7.891083 / 8 bit(s)

H_r: 7.891083
H_c: 7.891083
H_I: 7.963649

Validation Test Passed...

min(H_r, H_c, H_I): 7.891083
```

Figure 2: NIST Restart Tests and Entropy Validation for CS128M

BSI AIS 31: Standard Statistical Test Suite.

The BSI AIS 31 Standard Statistical Test Suite consists of nine independent tests to examine the randomness of binary sequences generated by the entropy source and the cryptographic post-processing algorithm. The evaluation process is broken into two test procedures, A and B. Test procedure A (Tests T0-T5) is applied to the post-processed final output of the RNG, or internal random numbers. Test procedure B (T6-T8) is applied to the raw output data of the entropy source. The goal is to ensure that the entropy per bit is sufficiently large prior to seeding the post-processing algorithm.

The complete testing suite, including documentation and software, can be downloaded directly from the BSI website[2]. A JAVA program is provided for simple use of the testing suite. The AIS 31 tests require large binary files of raw and internal random numbers, at least 3,145,728 bits for Test T0 and 5,140,000 bits for Tests T1-T5, to be tested. Binary files of raw and internal random data of 2 GB in length each were generated using our QNG Model CS128M (SN: QWR80001) to be analyzed.

For the generated random data file all of the statistical tests were applied and the result recorded in the following Table 5. In the case of the Test T8, Entropy Test, the bits of entropy per byte has been reported.

BSI AIS 31 Battery of Test Results	
Statistical Tests	**Results**
T0 – Disjointness Test	PASS
T1 – Monobit Test	PASS
T2 – Poker Test	PASS
T3 – Runs Test	PASS
T4 – Long Run Test	PASS
T5 – Autocorrelation Test	PASS
T6 – Uniform Distribution Test	PASS
T7 – Comparative Test for Multinomial Distributions	PASS
T8 – Entropy Test	PASS
T8 – Entropy Estimation (bits of entropy per byte)	7.997572

Table 5 — AIS 31 Test Suite Results for CS128M.

[2] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_testsuit_zip.zip

DIEHARD: A Battery of Tests of Randomness.

The DIEHARD Battery of Tests of Randomness, developed by Prof. George Marsaglia, contains a collection of 15 tests to examine the randomness of binary sequences generated by a TRNG or PRNG. The complete testing suite, including documentation and software, can be found from the DIEHARD archived website[3]. Windows executable files are provided for simple use of the testing suite. The DIEHARD tests require a large binary file of random integers, at least 80 million bits, to be tested. Therefore, a binary file of 80 million raw random bits in length was generated using our QNG Model CS128M (SN: QWR80001) to be analyzed.

For the generated random data file all of the statistical tests were applied and the resulting *p-values* recorded in the following Table 6. In the case of the Birthday Spacings, Binary Rank (6x8 matrices), OPSO, OQSO, DNA, Count-the-1's (specified bytes), This is a Parking Lot, The Minimum Distance, 3DSpheres, Overlapping Sums, and Runs (up & down) tests, only the K-S tests are reported here.

DIEHARD Battery of Tests Results	
Statistical Test	**p-value**
Birthday Spacings	0.544478
Overlapping 5-Permutation	0.627684
Binary Rank (31x31)	0.715902
Binary Rank (32x32)	0.977584
Binary Rank (6x8)	0.362809
Bitstream	0.255699
OPSO	0.083799
OQSO	0.788372
DNA	0.388282
Count-the-1's (byte stream)	0.848490
Count-the-1's (specified bytes)	0.822120
This is a Parking Lot	0.016155
The Minimum Distance	0.255680
3DSpheres	0.910887
Squeeze	0.067427
Overlapping Sums	0.501066
Runs (up)	0.646677
Runs (down)	0.217652
Craps (no. of wins)	0.919992
Craps (throws/game)	0.662403

Table 6 — DIEHARD Test Suite Results for CS128M.

[3] https://web.archive.org/web/20160113163414/http://stat.fsu.edu/pub/diehard/diehard.zip