ComScire QNG Model: PQ32MU
Validation Tests of Randomness

ComScire QNGmeter: Continuous Random Number Tester

The ComScire QNGmeter is a continuous statistical tester (Real-Time) 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 tens 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 PQ32MU 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(0) = p(1) = 0.5,

2) Auto Correlation - orders 1 up to 32, nominal expected value is 0.0 for all orders,

3) Entropy Test – nominal expected value is H = 1.0, an update of U. Maurer's "Universal Test" (J-S Coron, *LNCS*, Vol. 1560, pp29-42, 1999),

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) = 294.63 (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 65536 bits. The Serial test has a block size of 262144 bits. The Entropy test has 4194304 bits in a block. The OQSO test uses 10485775 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 hence 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 number. A meta KS test is finally calculated using the auto correlation KS result and the probabilities of the chi-squared results of the remaining tests. The meta KS(+) and KS(-) probabilities are displayed. Convergence toward 1.0 or 0.0 indicates failure.

If any cumulative z-score exceeds ± 4.265 standard deviations the generator will be determined as failed. Failure is also pronounced if the probability of any chi squared test is less than 0.00001 or greater than 0.99999, or if the probability of either of the Meta KS results is less than 0.0001 or greater than 0.9999.

For the hardware validation report, the QNGmeter tests were completed on a QNG Model PQ32MU for approximately 4.82 trillion random bits. All metatest results for the device are recorded in the following table.

ComScire QNGmeter 4.82 Trillion Bits Test

Testing QNG Device S/N QWR50011

Run Time Information	
Bits Tested	4.82E+12
Time Elapsed	3:16:45:00
Throughput	32.0E+06
Meter	40.1+
1/0 Balance	
p (z ≤ x)	0.930
p (χ2 ≤ x)	0.028
Entropy Test	
p (z ≤ x)	0.581
p (χ2 ≤ x)	0.421
Serial Test	
p (z ≤ x)	0.245
p (χ2 ≤ x)	0.492
OQSO (Monkey Test)	
p (z ≤ x)	0.573
p (χ2 ≤ x)	0.074
AC Meta KS- Test	
KS-	0.111
Meta KS Test	
KS+	0.949
KS-	0.031

Autocorrelation	
Order	p (χ2 ≤ x)
1	0.207
2	0.415
3	0.281
4	0.374
5	0.452
6	0.116
7	0.004
8	0.359
9	0.902
10	0.777
11	0.470
12	0.708
13	0.719
14	0.720
15	0.256
16	0.603
17	0.472
18	0.660
19	0.546
20	0.773
21	0.973
22	0.972
23	0.959
24	0.018
25	0.215
26	0.531
27	0.373
28	0.033
29	0.890
30	0.512
31	0.474
32	0.813