ComScire QNG Model PQ128MU
Validation Tests of Randomness

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 14.04. 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 80,000,000 bits in length was generated using our QNG Model PQ128MU (SN: QWR70004) to be analyzed.

All test results are recorded in the following Table 1. 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, only one of the possible 8 and 18 *P-values*, respectively, has been reported.

NIST Battery of Tests Results	
Statistical Test	**P-value**
Frequency	0.213309
Block Frequency (m = 128)	0.739918
Cumulative Sums-Forward	0.350485
Cumulative Sums-Reverse	0.017912
Runs	0.739918
Long Runs of Ones	0.739918
Rank	0.035174
Spectral DFT	0.122325
Non-overlapping Templates (m = 9)	0.073231
Overlapping Templates (m = 9)	0.534146
Universal	0.213309
Approximate Entropy (m = 10)	0.911413
Random Excursions (x = +1)	0.748177
Random Excursions Variant (x = -1)	0.041573
Linear Complexity (M = 500)	0.534146
Serial (m = 16, $\nabla\Psi^2_m$)	0.004301
Serial (m = 16, $\nabla^2\Psi^2_m$)	0.739918

Table 1— NIST Test Suite Results for PQ128MU.

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 directly from the DIEHARD website [1.]. 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 bits in length was generated using our QNG Model PQ128MU (SN: QWR70004) 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 2. 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 has been reported.

DIEHARD Battery of Tests Results	
Statistical Test	**P-value**
Birthday Spacings	0.026053
Overlapping 5-Permutation	0.717986
Binary Rank (31x31)	0.320859
Binary Rank (32x32)	0.394794
Binary Rank (6x8)	0.966855
Bitstream	0.878749
OPSO	0.682987
OQSO	0.561982
DNA	0.645468
Count-the-1's (byte stream)	0.745519
Count-the-1's (specified bytes)	0.089936
This is a Parking Lot	0.310429
The Minimum Distance	0.319546
3DSpheres	0.291031
Squeeze	0.476844
Overlapping Sums	0.701413
Runs (up)	0.303256
Runs (down)	0.071091
Craps (no. of wins)	0.623129
Craps (throws/game)	0.147330

Table 2— DIEHARD Test Suite Results for PQ128MU.

1. Link no longer provided by Florida State University. Test suite is available from alternate sites.