ComScire QNG Model R32MU
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 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 R32MU (SN: QWR30008) 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, 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	0.779188
Block Frequency (m = 128)	0.429923
Cumulative Sums-Forward	0.892036
Cumulative Sums-Reverse	0.792508
Runs	0.155499
Long Runs of Ones	0.809249
Rank	0.689019
Spectral DFT	0.406499
Non-overlapping Templates (m = 9)	0.733297
Overlapping Templates (m = 9)	0.919131
Universal	0.670396
Approximate Entropy (m = 10)	0.999170
Random Excursions	0.404546
Random Excursions Variant	0.379299
Linear Complexity (m = 500)	0.024028
Serial (m = 16, $\nabla\Psi^2_m$)	0.444691
Serial (m = 16, $\nabla^2\Psi^2_m$)	0.478839

Table 1— NIST Test Suite Results for R32MU.

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[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 raw random bits in length was generated using our QNG Model R32MU (SN: QWR30001) 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 are reported here.

DIEHARD Battery of Tests Results	
Statistical Test	**P-value**
Birthday Spacings	0.392871
Overlapping 5-Permutation	0.986152
Binary Rank (31x31)	0.790608
Binary Rank (32x32)	0.481808
Binary Rank (6x8)	0.865280
Bitstream	0.907780
OPSO	0.973809
OQSO	0.095557
DNA	0.328864
Count-the-1's (byte stream)	0.776809
Count-the-1's (specified bytes)	0.977505
This is a Parking Lot	0.862518
The Minimum Distance	0.448718
3DSpheres	0.394904
Squeeze	0.734519
Overlapping Sums	0.240960
Runs (up)	0.956689
Runs (down)	0.611432
Craps (no. of wins)	0.521652
Craps (throws/game)	0.240847

Table 2— DIEHARD Test Suite Results for R32MU.

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