

ComScire QNG Model R2000KU 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 , $\sqrt{2}$ and $\sqrt{3}$. 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 R2000KU (SN: QWR20141) 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	0.784927
Block Frequency (m = 128)	0.900569
Cumulative Sums-Forward	0.999286
Cumulative Sums-Reverse	0.731886
Runs	0.135720
Long Runs of Ones	0.618385
Rank	0.149495
Spectral DFT	0.365253
Non-overlapping Templates (m = 9)	0.653234
Overlapping Templates (m = 9)	0.870856
Universal	0.649612
Approximate Entropy (m = 10)	0.512137
Random Excursions	0.760036
Random Excursions Variant	0.551962
Linear Complexity (m = 500)	0.585209
Serial (m = 16, $\nabla\Psi_m^2$)	0.998474
Serial (m = 16, $\nabla^2\Psi_m^2$)	0.429923

Table 1— NIST Test Suite Results for R2000KU.

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 website¹. 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 R2000KU (SN: QWR20141) 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	0.853236
Overlapping 5-Permutation	0.826763
Binary Rank (31x31)	0.931721
Binary Rank (32x32)	0.961805
Binary Rank (6x8)	0.298009
Bitstream	0.831529
OPSO	0.595235
OQSO	0.292152
DNA	0.191343
Count-the-1's (byte stream)	0.564874
Count-the-1's (specified bytes)	0.414715
This is a Parking Lot	0.014159
The Minimum Distance	0.381348
3DSpheres	0.751597
Squeeze	0.670939
Overlapping Sums	0.146658
Runs (up)	0.918427
Runs (down)	0.251912
Craps (no. of wins)	0.493110
Craps (throws/game)	0.798057

Table 2— DIEHARD Test Suite Results for R2000KU.

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