ComScire QNG Model PQ32MU
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. In order to run the NIST STS, some modifications to the source code were necessary for the software to compile using Visual Studio 2008 running in a Windows Vista environment. These modifications consist of implementing the error (*erf*) and complementary error (*erfc*) functions that do not exist in the Microsoft's math library.

The Cephes C language special functions math library, already included in the NIST STS software, was used to implement the error and complementary error functions. All *erf* and *erfc* functions in the source code were replaced by *cephes_erf* and *cephes_erfc* functions, respectively. After the successful compilation of the source code, 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, two binary files of 80,000,000 and 1,000,000 bits in length were generated using our QNG Model PQ32MU (SN: QWR50001) to be analyzed. The generation of the 1Mb data file was necessary to run the Random Excursions, Random Excursions Variant, and Spectral DFT tests. These tests were unable to generate results when using the 80Mb data file. The warning messages for the Random Excursions and Random Excursions Variant tests were "Test not applicable. There are an insufficient number of cycles". The warning message for the Spectral test was "Unable to allocate working arrays for the DFT". Therefore, all tests except for Random Excursions, Random Excursions Variant, and Spectral DFT were applied for the 80Mb data file.

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	0.315166
Block Frequency (m = 128)	0.677159
Cumulative Sums-Forward	0.172339
Cumulative Sums-Reverse	0.486293
Runs	0.535586
Long Runs of Ones	0.590790
Rank	0.858419
Spectral DFT	0.479815
Non-overlapping Templates (m = 9)	0.762000
Overlapping Templates (m = 9)	0.077807
Universal	0.170289
Approximate Entropy (m = 10)	0.291253
Random Excursions (x = +1)	0.946962
Random Excursions Variant (x = -1)	0.393786
Linear Complexity (M = 500)	0.837092
Serial (m = 16, $\nabla\Psi^2_m$)	0.682535
Serial (m = 16, $\nabla^2\Psi^2_m$)	0.253212

Table 1— NIST Test Suite Results for PQ32MU.

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. 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, the same 80Mb data file used for the NIST STS battery of tests was used for the DIEHARD test.

For the 80Mb 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	0.584316
Overlapping 5-Permutation	0.023375
Binary Rank (31x31)	0.700515
Binary Rank (32x32)	0.703387
Binary Rank (6x8)	0.586651
Bitstream	0.512400
OPSO	0.852800
OQSO	0.235200
DNA	0.403800
Count-the-1's (byte stream)	0.800646
Count-the-1's (specified bytes)	0.251800
This is a Parking Lot	0.975336
The Minimum Distance	0.421422
3DSpheres	0.119535
Squeeze	0.813194
Overlapping Sums	0.102156
Runs (up)	0.612206
Runs (down)	0.039565
Craps (no. of wins)	0.611182
Craps (throws/game)	0.237462

Table 2— DIEHARD Test Suite Results for PQ32MU.