

Quantis

True randomness upon request



Quantis-OEM
(4 Mbits/sec)



Quantis-PCI
(up to 16 Mbits/sec)

RANDOMNESS TEST REPORT

id Quantique

Ch. de la Marbrerie, 3 1227 Carouge Switzerland
Tel: +41 (0)22 301 83 71 Fax: +41 (0)22 301 83 79
sales@idquantique.com
www.idquantique.com



A Quantum Leap for Cryptography

Quantis is a physical random number generator (RNG) that produces truly random numbers at a high bit rate of 4Mbits/sec. The randomness of the number generation process is guaranteed by the laws of quantum physics.

Introduction to random number generators

Random number generators (RNGs) can be grouped in three families:

Pseudo-random number generators

Software-based generators use an algorithm into which some initial value is fed to produce a sequence of pseudo-random numbers. Since the sequence they produce is always periodic, they should not be used in applications where randomness is required.

Physical random number generators based on a chaotic process

Macroscopic processes described by classical physics can be used to generate random numbers. Typical chaotic processes include the monitoring of some electric noise current in a resistor or in a diode. This current is not random, but just very complex to describe. Determinism is hidden behind complexity. Although their random numbers are likely to pass randomness tests, these generators are difficult to model. This implies that it is impossible to verify if they are operating properly while acquiring numbers. In addition, it is difficult to ensure that the system is not interacting with environment parameters like temperature or an electromagnetic field.

Physical random number generators based on a quantum process

Quantum physics is the only theory within the fabric of modern physics that integrates randomness. This fact was very disturbing to physicists like Einstein who invented quantum physics. However, its intrinsic randomness has been confirmed over and over again by theoretical and experimental research. Truly random numbers can be generated by monitoring radioactive decay of heavy elements. Although they produce numbers of excellent quality, such generators are not suitable for commercial applications. In 2001, *id Quantique* introduced the first commercial physical random number generator based on quantum physics. The randomness is guaranteed by the random behaviour of single 'light particles' - called photons - hitting a semi-transparent mirror. The process by which photons incident on such a component is either reflected or transmitted is intrinsically random and cannot be influenced by external parameters. The quantum process used to generate the random bits, its immunity to external factors, plus the fact that the Quantis unit performs live verifications of its internal functions, guarantees a high level of trust in the random numbers that are generated.

This document gives a brief overview of the tests that were performed to evaluate the randomness of the bit stream generated by the Quantis product. The most stringent randomness tests, namely the **NIST test** (issued by the National Institute of Standards and Technology, Special Publication 800-22) and the **DIEHARD test**, were performed. The Quantis random number generator successfully passed all randomness tests.

Randomness test suite 1: NIST

(<http://csrc.nist.gov/rng/>)

The NIST *statistical test suite for random number generators* offers a battery of 16 statistical tests. These tests assess the presence of a pattern which, if detected, would indicate that the sequence is non-random. The properties of a random sequence can be described in terms of probability. In each test a probability, called the p-value, is extracted. This value summarizes the strength of the evidence against the perfect randomness hypothesis. A p-value of zero indicates that the sequence appears to be completely non-random. A p-value larger than 0.01 means that the sequence is considered to be random with a confidence of 99%.

The following table shows typical results obtained on a series of 1 billion bits. The random data was generated by a Quantis module in about 4 minutes. The NIST test suite was performed on 1000 bit streams, each stream containing 1 million random bits. The mean and variance of the p-values are shown below:

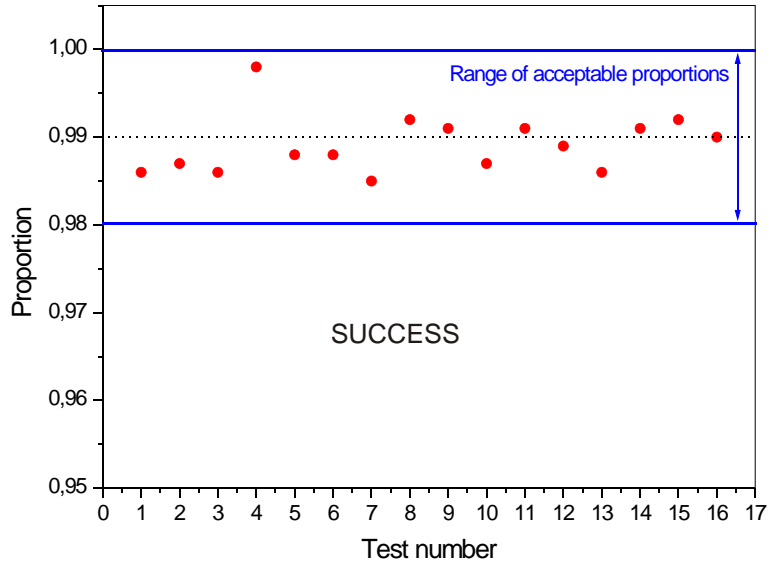
Test name	Mean of p-value	Variance	Conclusion
Approximate Entropy Test	0.489	0.088	SUCCESS
Frequency Test within a Block	0.506	0.081	SUCCESS
Cumulative Sums Test	0.499	0.081	SUCCESS
Discrete Fourier Transform (Spectral) Test	0.493	0.079	SUCCESS
Binary Matrix Rank Test	0.498	0.084	SUCCESS
Run Test	0.497	0.081	SUCCESS
Serial Test	0.495	0.078	SUCCESS
Maurer's Universal Statistical Test	0.493	0.081	SUCCESS
Linear Complexity Test	0.499	0.083	SUCCESS
Test for the Longest Run of Ones in a Block	0.503	0.087	SUCCESS
Non-overlapping Template Matching Test	0.499	0.082	SUCCESS
Overlapping Template Matching Test	0.490	0.081	SUCCESS
Frequency (Monobit) Test	0.505	0.084	SUCCESS
Lempel-Ziv Compression Test	0.480	0.080	SUCCESS
Random Excursions Test	0.503	0.083	SUCCESS
Random Excursions Variant Test	0.502	0.082	SUCCESS

The significance level for each test of the NIST SP800-22 test suite is set to 1%. A value called the *proportion* is extracted for each test. The proportion is the number of sequences having a p-value larger than 1%, divided by the number of binary sequences. For this test 1000 binary sequences of 1 million bits each was used.

The plot on the right shows the proportion for each of the 16 tests. NIST SP800-22 specifies a range of acceptable proportions. Since the proportion for each test is larger than 0.9805 and smaller than 0.9994, there is very high confidence that the data is truly random.

Further analysis has also confirmed that the distribution of the p-values is within the NIST SP800-22 specifications.

The bit stream generated by Quantis has therefore a high level of randomness.



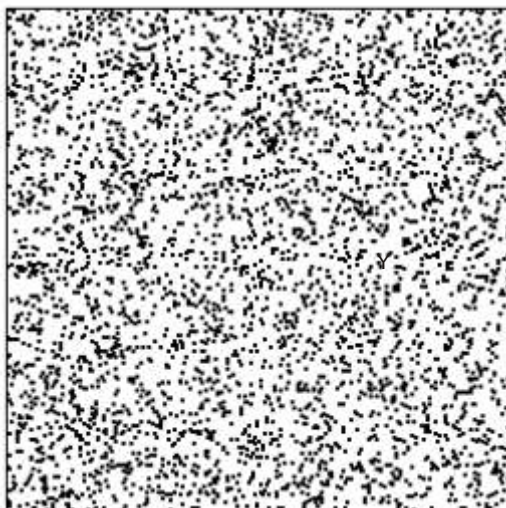
Randomness test suite 2: DIEHARD

(<http://www.csis.hku.hk/~diehard/cdrom/>)

The DIEHARD test suite is a battery of 18 stringent statistical tests. Large files of 1 billion bits each were generated with a Quantis module and the randomness of the data was tested using the DIEHARD test suite. The following table shows a typical result obtained on a single bit stream of 1 billion bits. A p-value larger than 0.01 and smaller than 0.99 means that the sequence is random with a confidence of 99%. All the tests that were performed on the Quantis modules have confirmed the high level of confidence in the randomness of the data.

Test name	p-value	Conclusion
Birthday Spacing Test	0.493	SUCCESS
Overlapping 5-Permutation Test	0.679	SUCCESS
Binary Rank Test (31x31 matrices)	0.692	SUCCESS
Binary Rank Test (32x32 matrices)	0.789	SUCCESS
Binary Rank Test (6x8 matrices)	0.730	SUCCESS
Bitstream Test	0.622	SUCCESS
Overlapping-Pairs-Sparse Occupancy Test	0.524	SUCCESS
Overlapping-Quadruples-Sparse-Occupancy Test	0.562	SUCCESS
DNA Test	0.657	SUCCESS
Count-the-1's Test (on stream of bytes)	0.418	SUCCESS
Count-the-1's Test (on specific bytes)	0.557	SUCCESS
Parking Lot Test	0.409	SUCCESS
Minimum Distance Test	0.551	SUCCESS
3D Spheres Test	0.681	SUCCESS
Squeeze Test	0.415	SUCCESS
Overlapping Sums Test	0.460	SUCCESS
Runs Test	0.698	SUCCESS

Two-dimensional scatter diagram



Randomness tests in production

As part of our quality insurance program, all Quantis-OEM modules and Quantis-PCI cards undergo a series of randomness tests before shipment to customers. The following randomness tests are being performed:

- Balancing Test
- Autocorrelation Test
- Maurer Universal Test
- Run Test
- Single level Serial Test
- Single Level Entropy Test
- Single Level Frequency Test

