Annex to METAS Certificate Nr. 151-04687

Object	**Quantum Random Number Generator** Quantis-USB S/N 070222A410 Quantis-PCI-1 S/N 08338A310 Quantis-PCI Express S/N 1002251A210
Applicant	**id Quantique SA** Ch. De la Marbrerie 3 1227 Carouge/Geneva Switzerland
Requirements	The output of the Quantis random number generator has to pass all DIEHARD Battery of Tests, confirming that the random number generator distributes numbers with sufficient non-predictability, fair distribution and lack of bias to particular outcomes. Specifically: 10 data sets consisting of 1E8 bits per data set is considered to be random if none of the 234 p-values produced by the 15 DIEHARD Battery of Tests has a value between 1 and 1-epsilon, where epsilon is 1e-6.
Date:	10 May 2010

1. Introduction

This annex describes the technical aspects of the tests performed on the Quantis-USB, Quantis-PCI-1 and Quantis-PCI Express quantum random number generators (RNG) using the DIEHARD Battery of Tests.

2. Output of the Quantis random number generator

The Quantis quantum random number generators are hardware based random number generators, producing a continuous stream of bits (0 or 1) at a rate of approximately 4 Mbits/s. Owing to the underlying quantum physical process of detecting single photons, this sequence of random bits is truly random.

The sequence of random bits generated cannot be predicted and cannot be reproduced.

3. The DIEHARD Battery of Tests

The DIEHARD Battery of Tests consists of 15 different, independent statistical tests. Results of tests are so called "p-values" which are between 0 and 1. For any given test, smaller p-value means better test result. An individual test is considered to be failed if p value approaches 1 closely, for example p>0.9999.

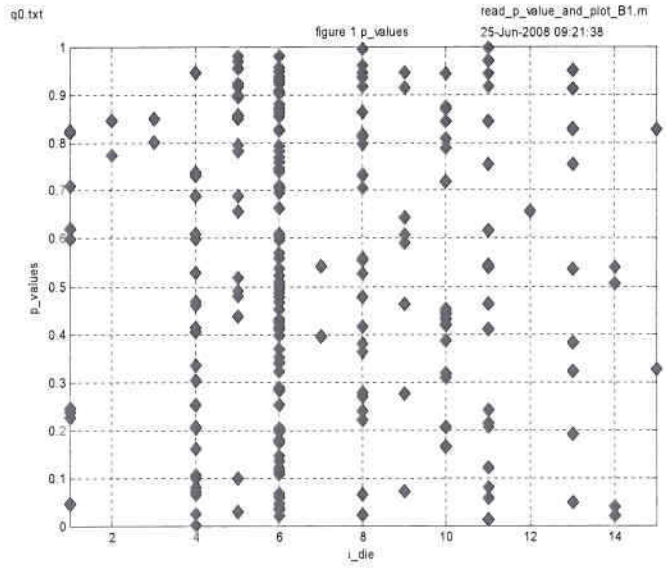
METAS
Lindenweg 50, CH-3003 Bern-Wabern, Tel. +41 31 32 33 111, www.metas.ch

The software is accessible at http://www.stat.fsu.edu/pub/diehard/

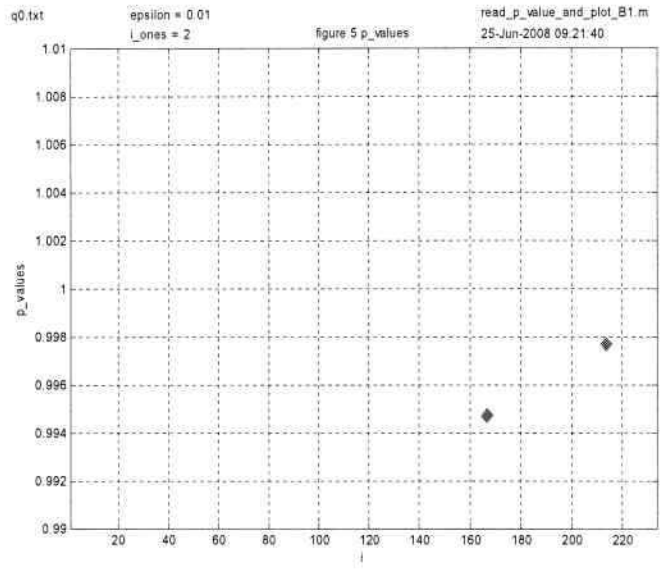
The DIEHARD Battery of Tests is currently considered to be the standard for evaluating the randomness of random number generators.
From the DIEHARD website the program DIEQUICK.EXE was used on 32-bit Pentium 4 (2.8 GHz) PC with Windows XP. The 15 statistical tests produce 234 different p-values which are organized as follows:

```
---------- q0.dat -------------------------

========= p_values of DIEHARD calculation no: 1  BIRTHDAY
0.599518  0.709861  0.237852  0.820910  0.619661
0.226836  0.823409  0.046390  0.245067
========= p_values of DIEHARD calculation no: 2  OPERM5
0.772826  0.844693
========= p_values of DIEHARD calculation no: 3  RANK MATRIX
0.800918  0.848990
========= p_values of DIEHARD calculation no: 4  RANK BITS
0.688477  0.730509  0.945024  0.460938  0.203490
0.302597  0.334386  0.610444  0.597908  0.469749
0.070558  0.204469  0.079579  0.000076  0.024039
0.252292  0.528699  0.161114  0.405471  0.736463
0.098169  0.414788  0.064616  0.104870  0.207195
========= p_values of DIEHARD calculation no: 5  MISSING WORDS
0.849500  0.855950  0.795030  0.979730  0.969630  0.915500  0.781500  0.028090  0.954340  0.921830
0.518330  0.688720  0.480130  0.895490  0.898000  0.436580  0.098440  0.656690  0.491310  0.853290
========= p_values of DIEHARD calculation no: 6  OPSO OQSO DNA
0.106400  0.536600  0.745700  0.341600  0.538000  0.339100  0.853300  0.936600  0.870700  0.477500
0.037500  0.709000  0.284300  0.197800  0.252500  0.902400  0.823800  0.173000  0.739000  0.827300
0.782800  0.948100  0.503700  0.452300  0.901000  0.569500  0.707000  0.021100  0.424300  0.144900
0.557500  0.467100  0.928800  0.416300  0.059700  0.352900  0.522500  0.369400  0.174500  0.411100
0.135800  0.510400  0.494100  0.922100  0.200900  0.057700  0.868800  0.605100  0.322000  0.020900
0.281800  0.879000  0.979500  0.180000  0.288300  0.862200  0.146600  0.485500  0.662000  0.769300
0.759300  0.955800  0.907200  0.693700  0.066900  0.610000  0.596300  0.114200  0.396100  0.035700
0.929800  0.060600  0.869300  0.045100  0.410900  0.431700  0.791900  0.033400  0.705000  0.408600
0.203300  0.121200
========= p_values of DIEHARD calculation no: 7  COUNT-THE-1s SUCC
0.540532  0.394400
========= p_values of DIEHARD calculation no: 8  COUNT-THE-1s SPEC
0.416352  0.811493  0.064476  0.219596  0.238661  0.476977  0.935159  0.730876  0.278049  0.553417
0.944694  0.797441  0.269171  0.862242  0.558111  0.916473  0.961669  0.815440  0.732429  0.706159
0.525874  0.021807  0.379471  0.362580  0.994698
========= p_values of DIEHARD calculation no: 9  CDPARK
0.607947  0.463618  0.642555  0.944998  0.071982  0.914635  0.590298  0.607947  0.071982  0.276387
========= p_values of DIEHARD calculation no: 10  MIN DIST
0.387044  0.418649  0.718532  0.441361  0.318943  0.431793  0.807295  0.164314  0.205480  0.844143
0.444977  0.788999  0.868265  0.452417  0.873407  0.419290  0.309323  0.943875  0.433578  0.418769
========= p_values of DIEHARD calculation no: 11  3DSPHERES
0.214670  0.616190  0.970930  0.241780  0.538980  0.754200  0.616350  0.056020  0.079230  0.462400
0.010900  0.206080  0.914990  0.844510  0.968650  0.121160  0.997700  0.409820  0.544580  0.943320
========= p_values of DIEHARD calculation no: 12  SQUEEZE
0.656615
========= p_values of DIEHARD calculation no: 13  OSUM
0.911757  0.047416  0.753983  0.322797  0.382270  0.536131  0.827740  0.825807  0.190067  0.949533
========= p_values of DIEHARD calculation no: 14  RUNS
0.506083  0.039519  0.538988  0.019816
========= p_values of DIEHARD calculation no: 15  CRAPS
0.327571  0.825604

-------------------------------------------------------------------------------------

q0.dat
epsilon = 0.1  i_zeros = 29  i_ones = 31
epsilon = 0.01  i_zeros = 1  i_ones = 2
epsilon = 0.001  i_zeros = 1  i_ones = 0
epsilon = 0.0001  i_zeros = 1  i_ones = 0
```

This set of p-value data is further analyzed by a MATLAB (Version 7.5.0342 / R2007b) program "read_p_value_and_plot_C1.m" which displays all the p-values for the 15 different DIEHARD statistical tests:



Then the p-values are counted in the range between 1 and 1-epsilon. The following figure shows the range between 1 and 1-epsilon, with epsilon=0.01 for illustration purposes:



We define the requirements for a set of random data to fulfil the DIEHARD Battery of Tests as follows:

Definition:

A data set of 1E8 bits is considered to be random if none of the 234 p-values produced by the 15 DIEHARD Battery of Tests has a value between 1 and 1-epsilon, where epsilon is 1e-6.

METAS
Lindenweg 50, CH-3003 Bern-Wabern, Tel. +41 31 32 33 111, www.metas.ch

4. Testing the sensitivity of the DIEHARD Tests by modifying the RNG raw data

For the purpose of the METAS Certificate of Conformity 151-04255 a short C++ program "P_change_bitset_32int_1.exe" was written which sets bits in a regular fashion into the RNG raw data. The purpose was to see at which levels the DIEHARD Battery of Tests begins to create p-values larger than 1-epsilon, where different values of epsilon were chosen down to 1e-6.

The following screen shot illustrates the modifications induced by the program on a small data set of 500 bytes for illustration purposes:

```
Program : P_change_bitset_32int_1.exe
date = Tue Jun 24 11:22:46 2008

file_name_in = p2.dat
file_name_out = p2_i0k10.dat

size_of_file = 500 bytes
number_of_bits = 4000 bits
MEMORY_SIZE = 100 bytes
number_of_steps = 5

sizeof(data_arr_in[0]) = 4
number_of_array_elements = 25

 1 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1 0   1853043085
(1)0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1 0   1853043085

 0 1 0 0 0 0 1 1 1 1 1 1 0 1 1 0 1 1 1 1 0 0 0 1 0 0 0 0 0 1 1 0   1620012994
(1)1 0 0 0 0 1 1 1 1 1 1 0 1 1 0 1 1 1 1 0 0 0 1 0 0 0 0 0 1 1 0   1620012995

 1 0 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 1 0 0 1 0 0 1 0 0 0 1 1 0 1   2972044929
(1)0 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 1 0 0 1 0 0 1 0 0 0 1 1 0 1   2972044929

 0 0 1 0 0 1 1 0 0 0 1 1 1 1 0 1 0 1 0 1 1 0 1 0 0 0 0 0 1 0 1 0   1348123748
(1)0 1 0 0 1 1 0 0 0 1 1 1 1 0 1 0 1 0 1 1 0 1 0 0 0 0 0 1 0 1 0   1348123749

 1 1 0 1 1 1 0 1 1 0 0 0 1 0 1 0 0 0 1 0 0 1 1 1 0 0 1 1 0 1 1 0   1826902459
(1)1 0 1 1 1 0 1 1 0 0 0 1 0 1 0 0 0 1 0 0 1 1 1 0 0 1 1 0 1 1 0   1826902459

 1 0 0 1 1 0 0 0 1 0 0 0 0 0 1 0 0 1 0 0 0 1 1 0 0 1 1 0 0 1 0 1   2791457049
(1)0 0 1 1 0 0 0 1 0 0 0 0 0 1 0 0 1 0 0 0 1 1 0 0 1 1 0 0 1 0 1   2791457049

 1 0 1 0 1 1 1 1 1 0 1 0 1 1 0 1 1 1 1 1 1 1 1 1 0 0 0 0 1 1 1 0 1   3095377397
(1)0 1 0 1 1 1 1 1 0 1 0 1 1 0 1 1 1 1 1 1 1 1 1 0 0 0 0 1 1 1 0 1   3095377397

 1 0 0 1 0 1 0 0 1 0 1 1 0 1 1 0 1 1 0 0 1 0 1 0 0 0 0 0 1 0 1 0   1347644713
(1)0 0 1 0 1 0 0 1 0 1 1 0 1 1 0 1 1 0 0 1 0 1 0 0 0 0 0 1 0 1 0   1347644713

 1 0 0 0 0 0 1 0 1 0 1 1 0 1 0 1 1 1 0 1 1 0 0 0 1 0 1 1 1 0 1 0   1562094913
(1)0 0 0 0 0 1 0 1 0 1 1 0 1 0 1 1 1 0 1 1 0 0 0 1 0 1 1 1 0 1 0   1562094913

 1 1 0 0 1 0 1 1 0 0 1 0 0 0 1 0 1 1 0 1 0 0 1 1 1 1 1 1 1 0 1 0   1607156947
(1)1 0 0 1 0 1 1 0 0 1 0 0 0 1 0 1 1 0 1 0 0 1 1 1 1 1 1 1 0 1 0   1607156947

bit_count = 4000
number_of_ones_1 = 2027
number_of_ones_2 = 2029
number_of_32int = 125

number_of_32int_mod = 10
```

number of bits produced by Quantis RNG

number of 32 bit integers

number of 32 bit integers in which bit 0 is set to 1

The output file name "p2_i0k10.dat" has the following notation:

p2: original unmodified Quantis raw RNG data

i0: setting bit to value "1" at position 0 of the 32-bit integer

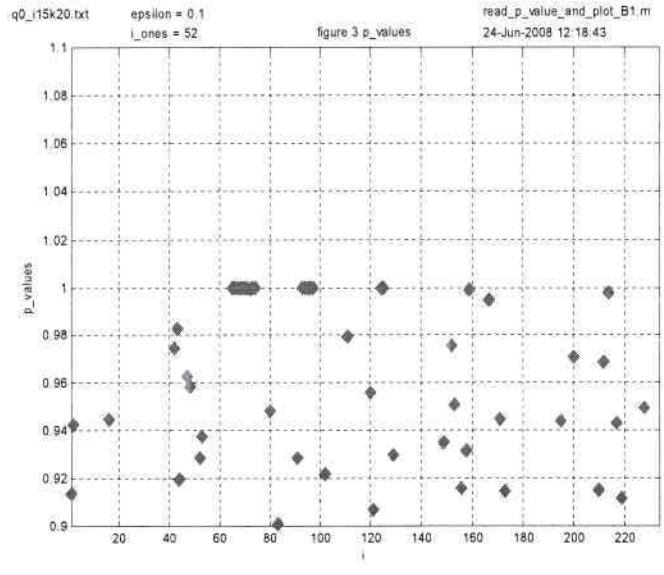
k10: repeat this for every k=10 32-bit integer.

METAS
Lindenweg 50, CH-3003 Bern-Wabern, Tel. +41 31 32 33 111, www.metas.ch

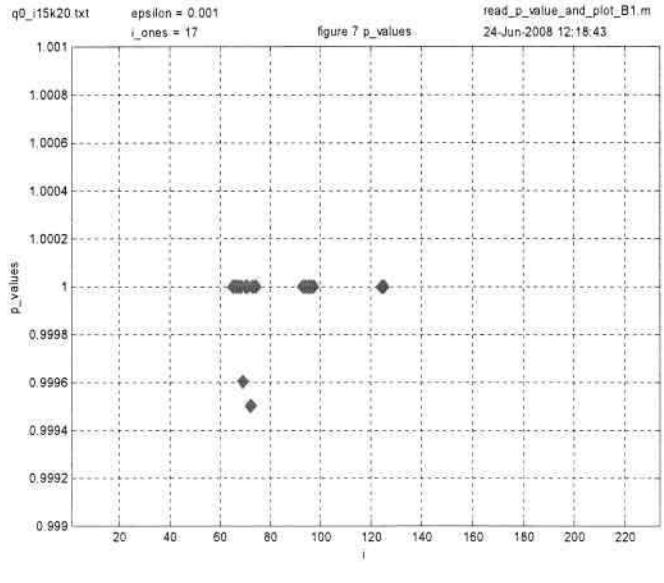
The following figure shows the p-values of the file "q0_i15k20.dat" in the range between 1 and 1-epsilon, where epsilon is 0.1.

The modified file "q0_i15k20.dat" consists of 100'000'000 bits of data which corresponds to 3'125'000 32-bit integers (12.5 Mbyte on disk).

At the bit position 15 every 20 th 32-bit integer has been set to the value "1".



The clustering of p-values close to 1 becomes evident if one displays the p-values in the range between 1 and 1-epsilon, where epsilon is 0.001.



METAS
Lindenweg 50, CH-3003 Bern-Wabern, Tel. +41 31 32 33 111, www.metas.ch

5. Results

The program DIEQUICK.EXE was performed on 10 sets of Quantis RNG generated random number data sets consisting of 100'000'000 bits (12.5 Mbyte): q0.dat - q9.dat.

The following table summarizes the results on the original raw data and the modified data as described in section 4.

All 10 data sets fulfill the definition of a random data set as defined in section 3:

A data set of 1E8 bits is considered to be random if none of the 234 p-values produced by the 15 DIEHARD Battery of Tests has a value between 1 and 1-epsilon, where epsilon is 1e-6.

From the table it is apparent that the first p-value close to 1 appears when the same bit is set in a 32-bit integer for every 40 th integer. When the number of repeating integers is decreased (e.g. every 20 th integer) the number of p-values close to 1 increases.

This confirms that the DIEHARD Battery of Tests is a viable measure for the randomness of a set of random number generators.

METAS
Lindenweg 50, CH-3003 Bern-Wabern, Tel. +41 31 32 33 111, www.metas.ch