



Tel: 0845 519 0154

+44(0)1276 510724

info@hdencrypt.com

Hawthorne Davies Limited

Paper 7: The Overlap Test of the Carousel Random Number Generator

Dr William McMullen Hawthorne

The Autocorrelation Test of Randomness is well established. A simple illustration of its working principle is as follows:

A sample of 50 binary numbers is arranged so that it is repeated and shifted by 4 places. The overlap is therefore 46 binary numbers in length. We now count the inequalities between both rows of the overlap:

```
10111010111000000010000010000100010001111010010011
  10111010111000000010000010000100010001111010010011
```

Inequalities

```
      x x  xxx  x   x x  xx          xxxx  xxxx  x
inequalities = 19
overlap = 46  inequalities/overlap = 0.41
                    expectation = 0.50
```

The sample is, of course, too small to allow a reliable inference to be made, and it would be totally unreliable if, for example, the overlap were reduced to 2. In order to test the Carousel Random Number Generator, we have modified the Autocorrelation Test and renamed it as the Overlap Test. To increase reliability we use an 8192 bit sample to measure 400 overlaps ranging from 8191 to 7792. Expectation:

$$\text{inequalities / overlap} = 50\%$$

OVERLAP (AUTOCORRELATION) TEST Sample size: 8192 bits
Expectation: Inequalities are 50% of the overlap. Starting point: 1596101
400 shifts.

```
50 50 50 51 50 50 50 51 50 50 50 50 50 48 50 50 50 50 49 50 51 50 50 50 50
50 50 50 50 49 50 50 51 51 50 50 50 51 50 50 50 49 50 51 50 50 50 50 49 51
51 50 50 49 51 50 50 51 50 50 50 50 51 51 50 50 50 50 51 51 51 51 50 50 50
49 49 50 50 49 50 50 50 49 50 49 49 50 50 51 50 50 51 50 50 50 50 49 50 50
49 50 49 51 50 50 51 51 49 50 50 50 50 50 50 49 49 50 50 51 51 50 50 50 50
50 50 50 50 50 50 49 51 50 50 50 50 51 50 50 49 49 50 49 51 48 50 50 50 51
49 49 51 50 51 51 50 49 50 50 50 50 50 50 50 50 50 51 50 50 50 51 51 50 51
50 49 50 50 49 51 50 51 50 50 50 50 50 50 50 50 49 49 49 51 51 51 50 49 51
50 50 49 50 50 50 51 50 50 50 49 50 50 49 50 51 50 50 50 49 50 49 50 49 51
50 50 50 50 50 50 52 50 50 50 50 50 50 50 51 49 50 49 50 49 51 49 50 50 50
51 49 50 51 51 49 50 51 49 50 50 51 50 50 50 49 50 50 50 49 50 51 51 50
51 51 49 50 50 50 51 50 50 49 50 50 50 50 49 50 51 51 50 50 49 49 50 50 50
50 49 50 51 50 50 51 49 49 49 50 51 50 49 49 50 51 51 50 50 50 51 50 50 49
50 50 50 51 51 50 49 50 50 49 50 51 50 49 49 50 50 51 51 50 50 50 50 51 50
50 50 51 50 50 50 50 51 49 49 49 50 51 51 50 50 49 50 51 50 50 50 50 51 50
50 50 50 50 51 50 49 51 50 50 49 50 50 51 49 49 50 49 50 50 49 51 50 50
```

This test has been repeated at many different starting points with equally consistent results.