

TEST REPORT SUMMARY

Issued By:	BMM Compliance Level 3, 810 Whitehorse Road Box Hill VIC 3128
Project Number:	UNIVERSAL.1001
Report Number:	SPINOMENAL.1001.01
Applicant:	Spinomenal 2014 LTD. Israel Bne Brak Baruh Hirsh 22
Reference Number:	N/A
Product Type:	Random Number Generator (RNG)
Product Name:	Online Gaming
Manufacturer:	Spinomenal 2014 LTD.
Standards Tested to:	GLI-19 – Interactive Gaming Systems
Issues / Observations:	None.
BMM Certification:	BMM certifies that the RNG used for Online Gaming complies with the requirements of GLI-19 – Interactive Gaming Systems for its intended purpose.

Box Hill, 17 Mar. 16

Signed:

Anna Fernando
VP Operations

The content of this document is strictly confidential. It has been prepared by BMM exclusively for Spinomenal 2014 Ltd. and relevant authorities and may not be disclosed to any other party without prior written approval of BMM.

BMM has conducted a level of testing which has historically been adequate for a submission of this type. However inherent in testing in a laboratory environment is the unavoidable limitation of it not being possible to verify that effects of all possible configurations and environments that occur in actual gaming venues

1. Purpose

Spinomenal 2014 LTD. has requested BMM to evaluate the random number generator (RNG) used in the Online Gaming against the requirements of GLI-19 – Interactive Gaming Systems.

2. Description of RNG

The RNG used is the RNGCryptoServiceProvider built into the .NET framework. It is an interface for the Windows CryptGenRandom function, which provides cryptographically secure random numbers. Although the exact implementation details are unknown, it is known to combine a SHA-1 algorithm with various hardware and software sources of entropy.

3. BMM Evaluation Performed

BMM examined the RNG source code and performed statistical tests on the output from the RNG.

3.1 Source Code Review

The CryptoRandom class provides a wrapper for an RNGCryptoServiceProvider instance. A static instance of the CryptoRandom class is used by all gaming sessions on the server. Static methods are also provided for drawing scaled numbers in desired target ranges without introducing any bias.

The underlying RNG is provided by the Windows CryptAPI and requires no seeding as it draws from the operating system's entropy pool. The state of the RNG can also not be saved or restored at any point. This is desirable, as the RNG's state must remain unknown and unpredictable at all times to maintain its security. The benefit of background cycling is also negated due to the cryptographic nature of the RNG, and as such is irrelevant for this type of RNG.

3.2 Statistical Testing

Statistical tests were performed on the output from the RNG. Sets of numbers of varying sizes from 500 to 5,000,000 in the ranges of 32, 52 and 111 were generated three times each and tested. One million 8-bit and 16-bit numbers were also generated for testing of the raw output from the RNG.

The following tests were performed on the data set:

- Frequency – frequency of each number across the entire sample set.
- Pairs Correlation – frequency of each pair of numbers occurring together.
- Gap – counts of the size of gaps between successive occurrences of numbers across the entire sample set.
- Coupon Collector – counts of how long it takes to collect complete sets of numbers.
- Runs – counts of ascending and descending sequences of numbers.
- Serial Correlation – counts of occurrences of pairs of numbers with specific gaps between them.
- Kolmogorov-Smirnov – test of the linear distribution of the chi-square probability results.
- Diehard tests – a suite of stringent tests on raw output from the RNG.

4. Test Results

The statistical tests on output from the RNG passed at the 99% confidence level. The following chart shows the distribution of test result probabilities and confirms their overall linearity.

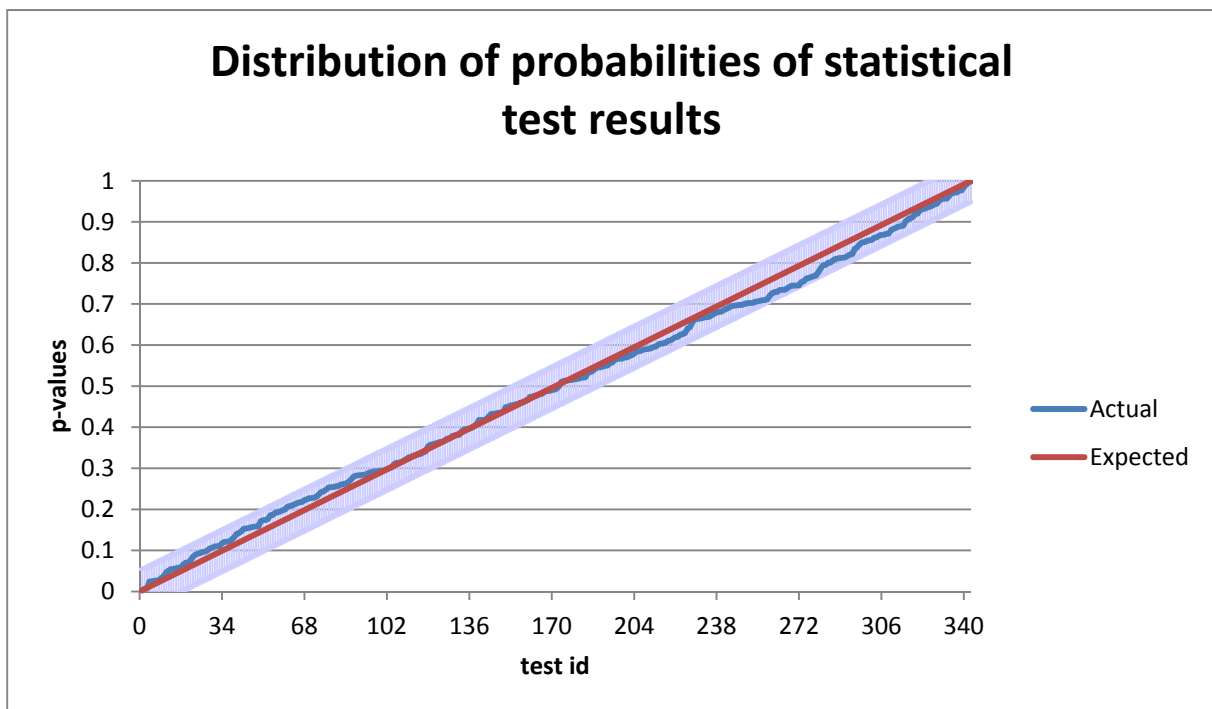


Figure 1: Distribution of probabilities of test results on output from the RNG

5. Conclusion

As a result of statistical testing and source code review, BMM believes that the RNG used by for Online Gaming provides uniformly random data suitable for its intended application. This RNG complies with the applicable requirements of GLI-19 – Interactive Gaming Systems.