



GLI[®]

GLI UK Gaming Ltd
Llys Helyg
Parc Menai
Bangor LL57 4EZ
United Kingdom

Tel: +44 (0)1248 660550
www.gaminglabs.com



4403

This report and any accompanying documents are provided "as is" with no warranties. All systems may contain defects and nothing in this document is intended to represent or warrant that any items assessed are complete and free from errors. The operator remains solely responsible for the design, functionality and provision of their product(s) and service(s), including any liability arising from legal infringement, technical non-compliance or product warranty. This document remains the property of GLI UK Gaming Ltd and, apart from supply to the intended regulator, is not to be copied, shared or distributed in any way without the express consent of GLI UK Gaming Ltd.

Worldwide Locations

World Headquarters
Lakewood, New Jersey

International Offices
GLI Africa
GLI Asia
GLI Australia Pty Ltd
GLI Austria GmbH
GLI Europe BV
GLI UK
GLI Italy
GLI South America

North American Offices
Colorado
Nevada
British Columbia

Report Type: TESTING REPORT

Issued by: GLI UK Gaming Ltd
Llys Helyg, Parc Menai, Bangor LL57 4EZ, United Kingdom

Evaluated by: GLI UK Gaming Ltd
Llys Helyg, Parc Menai, Bangor LL57 4EZ, United Kingdom
GLI UK Gaming Ltd
Llys y Fedwen, Parc Menai, Bangor LL57 4BL, United Kingdom

Recipient: Blueprint Gaming Ltd
Fortune House, Northgate Terrace, Northern Road, Newark-on-Trent NG24 2EU, United Kingdom

Jurisdiction: United Kingdom

Regulatory Documents: UK_TGA
The Gambling Act 2005 (April 2005)
UK_RTS
Remote gambling and software technical standards (June 2017)
UK_TSC
Testing strategy for compliance with remote gambling and software technical standards (November 2018)

Supplier: Blueprint Gaming Ltd
Fortune House, Northgate Terrace, Northern Road, Newark-on-Trent NG24 2EU, United Kingdom

Submitting Party: Blueprint Gaming Ltd
Fortune House, Northgate Terrace, Northern Road, Newark-on-Trent NG24 2EU, United Kingdom

Product Tested: Final Functionality Evaluation Report - Random Number Generator (RNG)

Evaluation Period: 01 October 2019 - 15 October 2019

Reference: RN/385/BPR/19/001/UK/RTS/01

Result: No issues are raised.

Authorised by:

Dr. Richard Edwards
Director

Table of Contents

Caveats	3
Test Item Details	4
Critical Components.....	4
RNG Evaluation	5
Scope.....	5
Technical Analysis.....	5
Empirical Testing.....	6
Summary.....	8
Assessment	9
Appendix	10

Caveats

The results presented in this document are a summary of the testing work undertaken. This report is subject to a number of caveats, including:

- All items provided for inspection and/or testing are declared by the customer to be configured identically to those in commercial use, with the exception of operator-configurable aspects that will not have a bearing on fairness and compliance.

All efforts have been taken to ensure that the testing undertaken was as exhaustive as necessary to demonstrate compliance or non-compliance. GLI UK Gaming Ltd (GLI UK) takes on trust that all test items (including all hardware and software), all documentation and all communications are accurate, truthful and that there is no intention to deceive or subvert the assessment of compliance.

Test Item Details

Critical Components

File name	SHA-1 checksum
BPRNG.dll	2082c17eca527ba76356d63c870dccf010f9b35b

RNG Evaluation

Scope

The random number generator (RNG) was assessed for suitability with Bingo, Blackjack games, Keno, Lotteries, Poker, Reels and Roulette gaming applications through static analysis of source code and statistical analysis of data generated using the supplied test utility.

The analysis undertaken is intended to confirm that the implementation and instantiation methods comply with the requirements of the jurisdictions in the scope of the assessment.

Technical Analysis

Manufacturer	Blueprint
Product	BPRandom
Version / serial number	V2.0.0.1
Platform supplier	N/A RNG-only test
Platform version	N/A RNG-only test
Type of RNG	Software
Random / pseudorandom	Pseudorandom
RNG shared	The RNG is shared by multiple games running on the same platform instance.
Coded language	C#
Algorithm	ISAAC
Bit depth	32 bits
Period	Average of 2^{8295} ; min of 2^{40}
Verified draw types	With / Without
Verified degrees of freedom (DoF)	0-36, 0-51, 0-255, 0-51V, 2^{32-2}
Location of data generation	Generated by GLI UK
Date of generation	02/10/2019, 07/10/2019
Threading	Single thread
Background cycling	Not present, is cryptographically strong and has background activity.
Cryptographic	Yes
Seeded securely	Yes

Empirical Testing

Please refer to the Appendices for details of the tests applied.

The test results are summarised as follows:

Analysis of 1 set of 32 million raw numbers between 0 and $2^{32} - 1$ (inclusive)

Test name	Sample size	Test result
Frequency (Monobits) Test	32,000,000	Pass
Frequency Test within a Block	32,000,000	Pass
Runs Test	32,000,000	Pass
Longest Run of Ones in a Block	32,000,000	Pass
Binary Matrix Rank Test	32,000,000	Pass
Discrete Fourier Transform (Spectral) Test	32,000,000	Pass
Non-overlapping Template Matching Test	32,000,000	Pass
Maurer's "Universal Statistical" Test	32,000,000	Pass
Linear Complexity Test	32,000,000	Pass
Serial Test	32,000,000	Pass
Approximate Entropy Test	32,000,000	Pass
Cumulative Sums (Cumsum) Test	32,000,000	Pass
Random Excursions Test	32,000,000	Pass
Random Excursions Variant Test	32,000,000	Pass

In summary, the data set passed the NIST suite of tests at the 95% confidence level, confirming that the software RNG is functioning correctly from a bitwise randomness perspective.

Analysis of 3 sets of 3 million raw numbers between 0 and $2^{32} - 1$ (inclusive)

Test name	Sample size	Test result
Birthday Spacing Test	3x 3,000,000	Pass
Overlapping 5-permutations Test	3x 3,000,000	Pass
Binary Rank 31x31 Test	3x 3,000,000	Pass
Binary Rank 32x32 Test	3x 3,000,000	Pass
Binary Rank 6x8 Test	3x 3,000,000	Pass
Bitstreams Test	3x 3,000,000	Pass
OPSO Test	3x 3,000,000	Pass
OQSO Test	3x 3,000,000	Pass
DNA Test	3x 3,000,000	Pass
Count the 1's (Specific Bytes) Test	3x 3,000,000	Pass
Count the 1's (Stream of Bytes) Test	3x 3,000,000	Pass
Parking Lot Test	3x 3,000,000	Pass
Minimum Distance Test	3x 3,000,000	Pass
3-D Spheres Test	3x 3,000,000	Pass
Squeeze Test	3x 3,000,000	Pass
Overlapping Sums Test	3x 3,000,000	Pass
Runs Test	3x 3,000,000	Pass
Craps Test	3x 3,000,000	Pass

In summary, the data set passed the Diehard suite of tests at the 99% confidence level, confirming that the software RNG is functioning correctly from a bitwise randomness perspective.

Analysis of 40 sets of 1 million scaled numbers between 0 and 36 (inclusive)

Test name	Sample size	Test result
Frequency Test (Equidistribution Test)	40,000,000	Pass
Serial Test (Non-overlapping Pairs)	40,000,000	Pass
Gap Test	40,000,000	Pass
Poker Test (Partition Test)	40,000,000	Pass
Permutation Test	40,000,000	Pass
Run Test	40,000,000	Pass

An additional assessment was applied across multiple sets of observations to ensure consistency with the expected behaviour of a high quality random number generator at the 95% confidence level. The frequency of occurrences of the possible outcomes was as expected for a random distribution and the outcomes covered the full range of possibilities.

Analysis of 40 sets of 1 million scaled numbers between 0 and 51 (inclusive)

Test name	Sample size	Test result
Frequency Test (Equidistribution Test)	40,000,000	Pass
Serial Test (Non-overlapping Pairs)	40,000,000	Pass
Gap Test	40,000,000	Pass
Poker Test (Partition Test)	40,000,000	Pass
Permutation Test	40,000,000	Pass
Run Test	40,000,000	Pass

An additional assessment was applied across multiple sets of observations to ensure consistency with the expected behaviour of a high quality random number generator at the 95% confidence level. The frequency of occurrences of the possible outcomes was as expected for a random distribution and the outcomes covered the full range of possibilities.

Analysis of 50 sets of 1 million scaled numbers between 0 and 255 (inclusive)

Test name	Sample size	Test result
Frequency Test (Equidistribution Test)	50,000,000	Pass
Serial Test (Non-overlapping Pairs)	50,000,000	Pass
Gap Test	50,000,000	Pass
Poker Test (Partition Test)	50,000,000	Pass
Permutation Test	50,000,000	Pass
Run Test	50,000,000	Pass

An additional assessment was applied across multiple sets of observations to ensure consistency with the expected behaviour of a high quality random number generator at the 95% confidence level. The frequency of occurrences of the possible outcomes was as expected for a random distribution and the outcomes covered the full range of possibilities.

Analysis of 1 million sets of shuffled numbers between 0 and 51 (inclusive)

Test name	Sample size	Test result
Frequency Test (Equidistribution Test)	1,000,000 shuffles	Pass
Serial Test (Non-overlapping Pairs)	1,000,000 shuffles	Pass
Gap Test	1,000,000 shuffles	Pass
Poker Test (Partition Test)	1,000,000 shuffles	Pass
Permutation Test	1,000,000 shuffles	Pass
Run Test	1,000,000 shuffles	Pass

An additional assessment was applied across multiple sets of observations to ensure consistency with the expected behaviour of a high quality random number generator at the 95% confidence level. The frequency of occurrences of the possible outcomes was as expected for a random distribution and the outcomes covered the full range of possibilities.

Summary

The RNG passed the NIST and DIEHARD bitwise tests for randomness. The RNG also passed a series of Knuth tests described in the appendices.

No deviations or biases were detected from the RNG in the generated data and the RNG is deemed suitable for the intended gaming applications.

Assessment

Section	Subsection	Compliant	Observation	Potential Issue	Not Applicable
UK_RTS RTS 7 – Generation of random outcomes	7A:1	✓			
	7A:2				✓ ^[01]
	7A:3				✓ ^[01]

[01] Out of scope.

Appendix

Empirical Test Methods

A number of empirical tests have been proposed to analyse frequencies of occurrence and localised correlations, patterns and intervals between generated numbers.

In this analysis, the following tests were used for raw RNG output:

NIST Test Suite

The following "bitwise" tests from the NIST Test Suite were applied:

- Frequency (Monobits) Test
- Frequency Test within a Block
- Runs Test
- Test for the Longest Run of Ones in a Block
- Binary Matrix Rank Test
- Discrete Fourier Transform (Spectral) Test
- Non-overlapping Template Matching Test
- Maurer's "Universal Statistical" Test
- Linear Complexity Test
- Serial Test
- Approximate Entropy Test
- Cumulative Sums (Cumsum) Test
- Random Excursions Test
- Random Excursions Variant Test

DIEHARD Battery of Tests

The following "bitwise" tests from the DIEHARD Battery of Tests of Randomness were applied:

- Birthday Spacing Test
- Overlapping 5-permutations Test
- Binary Rank 31x31 Test
- Binary Rank 32x32 Test
- Binary Rank 6x8 Test
- Bitstreams Test
- Overlapping Pairs Sparse Occupancy (OPSO) Test
- Overlapping Quadruples Sparse Occupancy (OQSO) Test
- DNA Test
- Count the 1's (Specific Bytes) Test
- Count the 1's (Stream of Bytes) Test
- Parking Lot Test
- Minimum Distance Test
- 3-D Spheres Test

- Squeeze Test
- Overlapping Sums Test
- Runs Test
- Craps Test

Donald Knuth's Empirical Tests for Randomness

The following tests were applied to the scaled and shuffled RNG outputs:

- Frequency Test (Equidistribution Test)
- Serial Test (Non-overlapping Pairs)
- Gap Test
- Poker Test (Partition Test)
- Permutation Test
- Run Test

All test results are based on the Pearson chi-squared test (also known as the chi-square "goodness of fit" test) to compare the observed results against expected outcomes and determine a level of confidence. For the following test descriptions, assume that a number n of uniformly distributed random numbers on the range $[0, m - 1]$, with m being an amount of distinct outcomes, were generated.

Frequency Test

The Frequency Test is designed to ensure that the random numbers are uniformly distributed throughout a given interval. The instances of each number in the range $[0, m-1]$ are counted and the counts compared to the expected populations. The probability P of observing any particular number x in a given position in the sequence is:

$$P(X) = \frac{1}{m}, \quad 0 \leq X \leq m - 1$$

The variation in observed distribution against the theoretical value is used to calculate the chi-squared statistic. The value of chi-squared statistic then maps to a probability (i.e. a p-value) that provides a measure of confidence in the observed outcomes.

Serial Test

The Serial Test checks that pairs of numbers are uniformly distributed in an independent manner. The random numbers are distributed into a number of equal bins and the frequencies of occurrence of all possible sequence pairs are checked (i.e. 0 followed by 0, 0 followed by 1, ..., $m - 1$ followed by $m - 1$). If the numbers are uncorrelated (i.e. no sequence pairs are favoured over any others), an equal distribution is expected and the probability of observing a sequence (x, y) is equal to:

$$P(x, y) = \frac{1}{m^2}, \quad 0 \leq x, y \leq m - 1$$

Similar to the frequency test, the observations and theoretical probabilities are used to compute a chi-squared statistic, which is then used to determine a probability that all serial pairs are uniformly distributed.

Gaps Test

The Gap Test considers the length of "gaps" between occurrences of specific numbers (i.e. the average gap between an occurrence of the number "1" and the next occurrence of "1" should be the same as that between a "2" and the next "2").

To apply the gap test, the lengths of the gaps between occurrences of a particular number are collated and the frequencies of occurrence are compared with the expected counts for each gap size. If subsequent numbers in the sequence are random and independent, the probability of a gap of length g , between instances of a particular output with probability $p = \frac{1}{m}$ occurring is:

$$P(g) = p(1 - p)^g$$

All gaps larger than a pre-determined threshold are grouped into a single category and counted. The probability of observing a gap of length u or larger is:

$$\sum_{g=u}^{\infty} P(g) = (1 - p)^u$$

A comparison of the observed and the expected gap sizes (via the chi-squared test) is then applied to assess if the sequence was generated by a sufficiently random source.

Poker Test

The Poker Test uses the analogy of a five-card hand in a poker game. It considers groups of five successive integers and observes which of the following 5 patterns is matched by each quintuple:

- 5 values (all different)
- 4 values (one pair)
- 3 values (two pairs or three of a kind)
- 2 values (full house or 4 of a kind)
- 1 value (five of a kind)

If each individual outcome is equally probable, the probability of achieving v distinct outcomes (in a group of k outcomes with d possible outcomes) is given by:

$$P(v) = S(k, v) \times \left(\frac{d(d-1) \cdots (d-v+1)}{d^k} \right)$$

where $S(k, v)$ is the Stirling Number of the second kind (the number of ways to partition a set of k elements into v non-empty subsets).

To apply the Poker Test, the generated random numbers are gathered into groups and categorised according the patterns listed above. The counts of each categorisation are compared with expected values via the chi-squared test.

Permutation Test

The Permutations Test divides a number sequence with a range of m elements into n groups of t elements. In this specific application, groups of $t = 3$ numbers were considered (denoted a, b, c) and counted the occurrence of each of the 6 different relative orderings:

- $a < b < c$
- $a < c < b$
- $b < a < c$
- $b < c < a$
- $c < a < b$
- $c < b < a$

The cases where two or more of the three numbers in a group are equal are also counted. The probability P^* that two or more of the instances are equal is given by:

$$P^* = \frac{1}{m} + \frac{2(m-1)}{m^2}$$

Hence, the probability of observing any of the listed permutations (lp) is:

$$P(lp) = \frac{(1 - P^*)}{3!}$$

A chi-squared test is conducted to test whether the observed counts of the permutations (including the matching cases) is consistent with the theoretical distribution.

Run Test

A sequence of random numbers will typically contain sub-sequences in which the numbers are increasing (they "run up") and sub-sequences in which they are decreasing (they "run down"). In this test, the sequence is split into segments in which the length is determined by whether or not the next number is higher (in the case of "run up"), or lower (in the case of "run down"). The number immediately following a run is discarded in order to make runs independent and make the chi-square test applicable. The observed value is then compared with the theoretical value and a level of confidence is calculated. Consider a sequence of uniformly distributed random numbers with m possible individual outcomes. The expected probability of a run of r consecutive numbers is:

$$P(r) = \begin{cases} m^r \binom{m}{r} - m^{-(r+1)} \binom{m}{r+1} & \text{if } 0 < r < m \\ m^{-m} & \text{if } r = m \end{cases}$$

The number of independent runs of each length up to and including m are compiled and compared with the expected values via a chi-squared goodness-of-fit test.

References:

- Bassham, L., Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., Vo, S. (2010) *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* [Online] v1a. Gaithersburg, MD, USA. National Institute of Standards & Technology. Available: <http://csrc.nist.gov/publications/details/sp/800-22/rev-1a/final>
- Knuth, D. (1997). *The Art of Computer Programming, Volume 2 (3rd Ed.): Seminumerical Algorithms* Boston: Addison-Wesley Longman Publishing Co, Inc.

END OF REPORT