bmm testlabs

TEST REPORT

Jurisdiction:	Malta
Authority:	Malta Gaming Authority
Customer:	Microslot [redacted]
Manufacturer:	Microslot
Submission Reference:	1 July 2024
Evaluated Product:	Online Random Number Generator (RNG) algorithm
Issued By:	BMM Testlabs
Location(s) of Evaluation:	BMM Testlabs Level 3, 810 Whitehorse Road Box Hill, Victoria 3128 Australia
Project Number:	QSP.1001
Report Number:	QSP.1001.01
Date of Issue:	15 August 2024
Date(s) of Evaluation:	2 August 2024
Standards Tested:	Malta: Remote Gaming Regulations (S.L.438.04)
Compliance Certification:	BMM hereby certifies that the Online Random Number Generator (RNG) algorithm complies with the standards listed above.
Signed:	
	Nikolas Putra, System Consultant, Mathematics

1. PURPOSE:

Microslot has requested BMM to evaluate the random number generator (RNG) used in the Online Random Number Generator (RNG) algorithm for operation in Malta**.**

2. EVALUATION METHOD:

The evaluation was conducted using the BMM testing procedures designed to ensure compliance to the applicable technical standards.

The full details of the tests are stored in the Quality Management System.

3. DESCRIPTION OF RNG:

The RNG uses the crypto module in Node.js which uses OpenSSL's RAND_bytes method that has the underlying AES-256 CTR-DRBG algorithm. The system is run on Ubuntu - 20.04.3 LTS.

3.1 SOURCE CODE REVIEW:

The following sections describe the implementation of the RNG in the source code.

3.1.1 Seeding

The underlying RNG seeds itself internally with entropy drawn from various system source.

3.1.2 Unpredictability

A secure algorithm is used, ensuring that it is infeasible to guess or determine the current RNG state, and hence all future output, by examining previous output. Entropy is continuously collected from various system sources and mixed into the RNG state to maintain security, even in the unlikely event that the state is somehow known.

3.1.3 Scaling

Methods are provided for drawing random values in usable ranges from a uniform distribution without introducing bias.

4. FILE SIGNATURES:

The following file(s) are used by the RNG.

File	Signature
CSPRNG.js	B23FAD406EFE03747633DCF32A0DA86D459710B5

5. STATISTICAL TEST RESULTS:

Each test tests the hypothesis that the RNG is a random source of numbers. A "p-value" is produced for each test run, which is the probability that a truly random process would produce the same or a more extreme result. P-values are expected to be uniformly distributed between 0 and 1. Each test is performed at least 100 times, and the p-values for each test are evaluated using an Anderson-Darling test. This produces a single p-value, which is the probability that the individual p-values have been produced from a uniform distribution.

Finally, the p-values from each test in the same test suite are combined using the Holm-Bonferroni method to provide an overall p-value. This process adjusts each p-value to ensure that the overall probability of accepting the RNG as random matches the confidence interval used. The overall p-value, equal to the minimum of the adjusted p-values, is compared to a specific alpha value to determine if the RNG is accepted or rejected as being random for a specific confidence interval. For a 99% confidence interval, the alpha value used is 0.01.

The following tables summarise the test results. See Appendix A for a description of the statistical tests used.

5.1 EMPIRICAL TESTS

Test	P-values	99% Confidence
Frequency Test	1.000000	PASS
Serial Correlation Test	0.481240	PASS
Runs Test	1.000000	PASS
Gap Test	1.000000	PASS
Coupon Collector Test	1.000000	PASS
Subsequences Test	1.000000	PASS
Poker Test	1.000000	PASS
Overall	**0.481240**	**PASS**

Conclusion: The RNG is **ACCEPTED** as random at the 99% confidence interval.

5.2 DIEHARD TESTS

Test	P-values	99% Confidence
Binary Rank 32x32 Test	1.000000	PASS
Binary Rank 6x8 Test	1.000000	PASS
Birthday Spacings Test	1.000000	PASS
Bitstream Test	1.000000	PASS
Count The 1's Stream Test	1.000000	PASS
Count The 1's Specific Test	1.000000	PASS
Runs Test	1.000000	PASS
Squeeze Test	0.208331	PASS
Overall	**0.208331**	**PASS**

Conclusion: The RNG is **ACCEPTED** as random at the 99% confidence interval.

5.3 NIST TESTS

Test	P-values	99% Confidence
Approximate Entropy Test	1.000000	PASS
Block Frequency Test	1.000000	PASS
Cumulative Sums Test	1.000000	PASS
Discrete Fourier Transform Test	1.000000	PASS
Frequency Test	1.000000	PASS
Linear Complexity Test	1.000000	PASS
Longest Run of Ones Test	1.000000	PASS
Non-Overlapping Template Matchings Test	1.000000	PASS
Overlapping Template Matchings Test	1.000000	PASS
Random Excursions Test	1.000000	PASS
Random Excursions Variant Test	1.000000	PASS
Rank Test	1.000000	PASS
Runs Test	0.869125	PASS
Serial Test	1.000000	PASS
Universal Test	1.000000	PASS
Overall	**0.869125**	**PASS**

Conclusion: The RNG is **ACCEPTED** as random at the 99% confidence interval.

6. NON-COMPLIANCES:

None.

7. CONDITIONS:

None.

8. ADDITIONAL INFORMATION:

1. If the above Online Random Number Generator (RNG) algorithm requires any parameters in order to be configured for operation in the field the parameters must be those which are specified by the manufacturer and must comply with the jurisdictional/operational requirements.

9. CONCLUSION:

As a result of statistical testing and source code review, BMM believes that the Online Random Number Generator (RNG) algorithm provides uniformly random data suitable for its intended application. This RNG complies with the applicable requirements for operation in Malta.

10. TERMS AND CONDITIONS:

BMM Testlabs ("BMM") has conducted a level of testing of the gaming product which has historically been adequate for a submission of this type. However, inherent in testing in a laboratory environment are the unavoidable limitations of not being able to verify the effects of all possible configurations and environments that occur in actual gaming venues.

This test report is for use by the client for the jurisdiction ("Jurisdiction") referenced in the report (the "Report") and only verifies, as of the date stated, the gaming product described in the Report subject to any conditions or limitations set forth therein.

The manufacturer named in the Report is solely responsible for possession of the appropriate license to sell, lease, service, or provide gaming supplies or gaming-related services in the Jurisdiction and for compliance with the ongoing requirements of the Jurisdiction. It is the responsibility of the manufacturer and operators to ensure that the gaming product detailed in this Report is installed, maintained and operated correctly without defects and safely in accordance with requirements of the Jurisdiction.

The Report and testing performed by BMM is proprietary to BMM. This Report is issued solely for the benefit of the client and shall not be reproduced, reprinted, or transmitted in whole or in part to any party not named in the Report without the written approval of BMM, other than by a regulator of the Jurisdiction. No third party may use, rely, or refer to the Report, its contents, or any related documents, without written permission of BMM. If BMM grants consent, BMM will send this Report via email as directed. BMM takes precautionary measures to secure the "PDF" document, but BMM does not send the email via any encrypted methodology.

The undersigned certifies under penalty of perjury that the compliance testing of the gaming product detailed in this Report and any accompanying documents was conducted in accordance with the requirements of the Jurisdiction and that the gaming product meets the requirements of its laws and the regulations adopted thereunder, and all published technical standards, control standards, control procedures, policies, industry notices and similar requirements implemented or issued by the Jurisdiction to the best of BMM's knowledge and belief.

Notwithstanding the above, any regulator may reprint, reproduce and transmit any document or information to any party that the regulator, in their sole discretion, deems appropriate.

BMM DOES NOT MAKE, AND EXPRESSLY DISCLAIMS, ALL OTHER WARRANTIES OF ANY KIND, EXPRESSED OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, SUITABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE LIABILITY AND OBLIGATIONS OF BMM HEREUNDER, AND THE REMEDY OF THE RECIPIENT, UNDER OR IN CONNECTION WITH THIS AGREEMENT SHALL BE LIMITED TO, AT BMM'S OPTION, REPLACEMENT OF THE SERVICES PROVIDED OR THE REFUND BY BMM OF ANY MONIES RECEIVED BY IT FOR THE SERVICES PROVIDED. IN NO EVENT SHALL BMM BE RESPONSIBLE TO THE CLIENT OR ANY THIRD PARTY FOR ANY CONSEQUENTIAL, INCIDENTAL, DIRECT, INDIRECT, OR SPECIAL DAMAGES, INCLUDING WITHOUT LIMITATION DAMAGES FOR LOST PROFITS OR REVENUE, BUSINESS INTERRUPTION, OR PUNITIVE DAMAGES, EVEN IF BMM HAD BEEN ADVISED OF THE POTENTIAL FOR SUCH DAMAGES.

APPENDIX A. STATISTICAL TESTS

The following tests were used to test the statistical properties of the RNG.

A1. EMPIRICAL TESTS

The Empirical Tests are based on the tests described by Donald Knuth in The Art of Computer Programming Volume 2: Seminumerical Algorithms (1968, revised in 1997). They test sequences of numbers scaled to specific ranges.

Frequency Test	Counts of each number occurring across the sample set.
Serial Correlation Test	Counts of non-overlapping groups of numbers occurring together. Group sizes of two, three, and four are tested separately.
Runs Test	Counts of ascending and descending sequences of numbers. Note that this is a different test to the Runs Test in the Diehard and NIST Tests.
Gap Test	Counts of the size of gaps between successive occurrences of a given number. Each number in the range is tested separately.
Coupon Collector Test	Counts of sequence lengths required to complete a full set of each number in the range.
Subsequences Test	Similar to the Serial Correlation Test for pairs of numbers, except looking at numbers separated by a specific gap. Step sizes of 5, 10, 15, and 20 are tested separately.
Poker Test	The sequence is split into groups of five. The number of unique values in each group is counted.

A2. DIEHARD TESTS

The Diehard Tests are based on the test suite published by George Marsaglia in 1995. They test sequences of raw binary output from the RNG.

Binary Rank 32x32 Test	Matrices are created using 32 32-bit words. The ranks of the resulting matrices are counted.
Binary Rank 6x8 Test	Same as the Binary Rank 32x32 Test, except each matrix is formed using 6 values, each taking 8 bits from successive 32-bit words with a specific offset. All possible offsets are tested separately.
Birthday Spacings Test	32-bit words are taken as values, sorted, and the spacings between them calculated. The number of spacings of the same size are counted.
Bitstream Test	Blocks of 2^18 values are treated as a stream of overlapping 20-bit values. The number of possible 20-bit values that are not found in each block is counted.
Count The 1's Stream Test	8-bit values are taken and assigned a “letter” based on the number of one’s appearing in the binary representation of each value. Overlapping groups of 5 “letters” are counted.
Count The 1's Specific Test	Similar to the Count The 1’s Stream Test, except 8-bit values are taken from successive 32-bit words with a specific offset. All possible offsets are tested separately.
Runs Test	Counts sequences of increasing and decreasing 32-bit words. Note that this is a different test to the Runs Test in the Empirical and NIST Tests.
Squeeze Test	A value of 2^31 is repeatedly multiplied by 32-bit words, dividing by 2^32 and taking the ceiling of the result each time. The number of successive words that are required to reduce the value down to 1 is counted. The value is reset to 2^31 and the process is repeated.

A3. NIST TESTS

The NIST Tests are based on the suite of tests released by the National Institute of Standards and Technology in Special Publication 800-22, Revision 1a (revised April 2010). They test sequences of raw binary output from the RNG.

Approximate Entropy Test	Similar to the Serial Test, count each possible m-bit value, except it does so for two adjacent m bit lengths and compares the two.
Block Frequency Test	Similar to the Frequency Test, except the data is split into equally sized blocks. The number of ones and zeroes in each block is counted.
Cumulative Sums Test	Random walks are created by converting the data to +1 / -1 for 1 / 0 respectively and summing consecutive values.
Discrete Fourier Transform Test	The data is transformed using a Discrete Fourier Transform. The number of peaks within the 95% threshold are counted.
Frequency Test	The number of ones and zeroes in the binary output is counted.
Linear Complexity Test	The length of the linear complexity of the random sequence is determined.
Longest Run of Ones Test	The data is split into equally sized blocks. The longest run of ones in each block is determined and counted.
Non-Overlapping Template Matchings Test	The data is split into equally sized blocks. Each block is searched for a specific pattern of bits and counted. A separate test is run for various bit patterns. Each bit pattern searched does not overlap with itself. That is, when the pattern is matched, the end of the pattern cannot be the start of another match.
Overlapping Template Matchings Test	Similar to the Non-Overlapping Template Matchings Test, except only one pattern is searched, which may overlap with itself.
Random Excursions Test	As with the Cumulative Sums Test, random walks are created by converting the data to +1 / -1 for 1 / 0 respectively and summing consecutive values. The number of times a given state is visited between returns to zero are counted. Separate tests are run for various states from -4 to +4, not including 0.
Random Excursions Variant Test	Similar to the Random Excursions Test, except the number of times the given state is visited is counted for the entire sequence. Separate tests are run for various states from -9 to +9, not including 0.
Rank Test	Matrices are created using 32 32-bit words. The ranks of the resulting matrices are counted. Note that this is fundamentally the same test as the Binary Rank 32x32 Test in the Diehard Tests, although the implementation may differ.
Runs Test	Runs of consecutive bits of the same value of various lengths are counted.
Serial Test	Counts of each possible m-bit values. Separate tests are run for various m bit lengths.
Universal Test	Distances between repeated patterns of bits are counted.

--- END OF REPORT ---