TEST REPORT SUMMARY

Client:	Gameplay Interactive Limited Akara Building 24 de Castro Street Wickhams Cay 1 Road Town Tortola British Virgin Islands
Machine Type:	Random Number Generator
Product Name:	Online Gaming
Date of Issue:	20 January 2016
Project Number:	GAMEPLAY.1002
BMM Test Report:	GAMEPLAY.1002.01
Market:	Online
Regulator:	N/A
Standards Tested to:	GLI-19: Interactive Gaming Systems Version 2.0
Issues/Observations:	None
BMM Certification:	I, Christopher van Prooije, Systems Consultant, Mathematics, hereby certify that the Random Number Generator used in Online Gaming complies with the relevant standards and is recommended for approval by the relevant authority for operation.
Signed:	**Christopher van Prooije, Systems Consultant, Mathematics**

NATA Accredited Laboratory
Number: 15122

Accredited for compliance with ISO/IEC 17025. The results of the tests, calibrations and/or measurements included in this document are traceable to Australian/National Standards.

1 PURPOSE OF EVALUATION

Gameplay Interactive Limited has requested BMM to evaluate the random number generator (RNG) used in Online Gaming against GLI-19: Interactive Gaming Systems Version 2.0.

2 DESCRIPTION OF RNG

The RNG draws numbers from a ComScire PQ32MU Quantum Number Generator (QNG) which creates random bits based on noise in MOS transistors and other sources of entropy. This is a true random number generator as it does not use a deterministic algorithm on an internal state to determine its next output, but relies on truly random physical events. As such, it is considered cryptographically secure, as there is no way to determine future or past numbers generated, regardless of how many bits from the RNG's output are observed.

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

An interface with the QNG is supplied through a C# class (Lottery.Helper.Random.HardwareGenerator, see Section 5 for the relevant source code files) and can be used to draw random integers or floating point numbers, scaling as required without introducing bias. As there is no internal state, there is no seeding or background cycling required. Ongoing monitoring of the QNG's output is conducted by the device itself to ensure it is operating correctly.

3.2 Statistical Testing

Statistical tests were performed on sample output from simulations of lottery games, where 20 numbers are drawn without replacement from a pool of 80 numbers. Five sets of samples were generated, containing a total of 22,541,273 sample game results between them.

The following tests were performed on the data set:

- Frequency Test – frequency of each number across the entire sample set.
- Gap Test – counts of the size of gaps between occurrences of specific numbers across the entire sample set.
- Coupon Test – counts of how long it takes to collect a complete set of numbers.
- Sum Frequency – frequency of total sums taken for each game set.
- Sum Runs – count of ascending and descending sequences of total sums taken for each game set.
- Column Frequency – frequency of each number in a specific position in each game set. For example, the seventh number drawn for each game.
- Column Sequential – frequency of each combination of two, three or four numbers occurring in the same position across successive games for specific positions in each game set.
- Column Gap – counts of the size of gaps between occurrences of specific numbers in the same position for specific positions in each game set.
- Column Runs – counts of ascending and descending sequences of numbers for specific positions in each game set.
- Column Coupon Collection – counts of how long it takes to collect a complete set of numbers for specific positions in each game set.
- Column Serial Correlation – counts of occurrences of pairs of numbers with specific gaps between them for each position in the game results.
- Diagonal tests – same as the column tests, but taking numbers from positions that shift left to right from one game set to the next. For example, taking the first number drawn in the first game, the second number drawn in the second game, and so on.
- Kolmogorov-Smirnov – test of the linear distribution of the chi-square probability results.

4 TEST RESULTS

The statistical tests on the game results generated with the RNG passed at the 99% confidence level. The following charts show the distributions of test result probabilities and confirm their overall linearity.

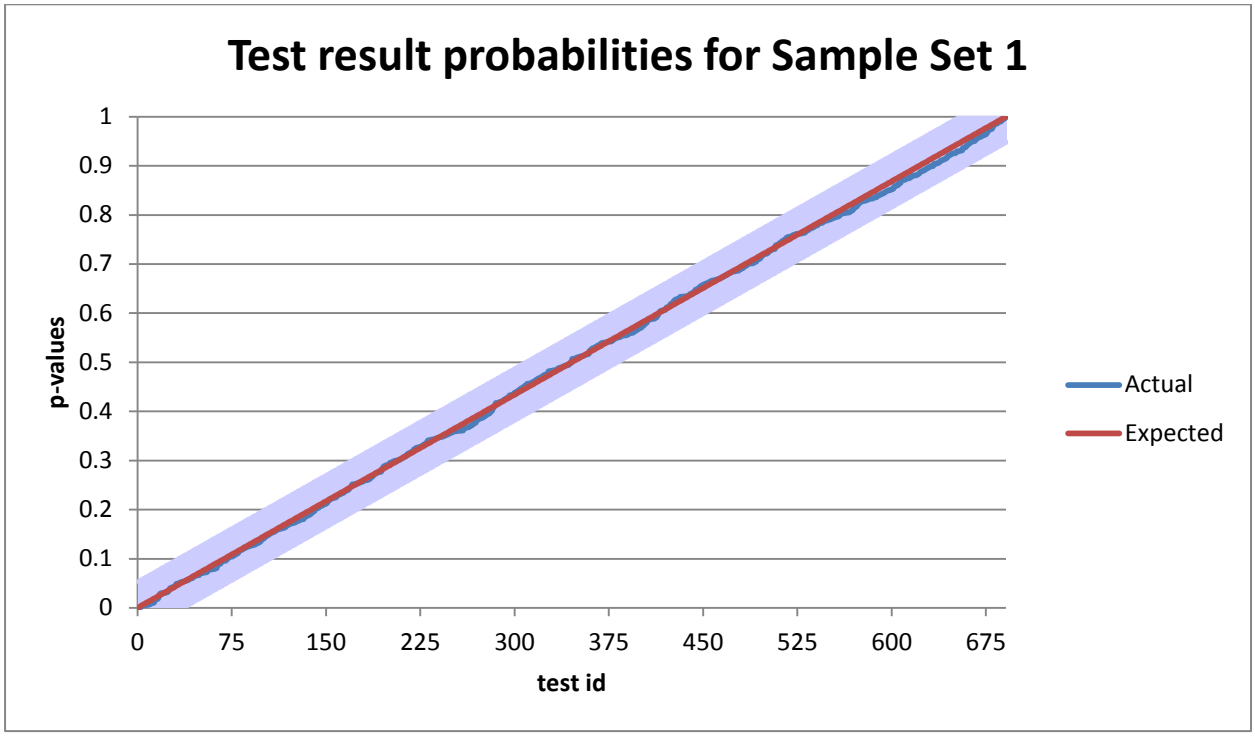

Figure 1: Distribution of result probabilities of tests on sample set 1

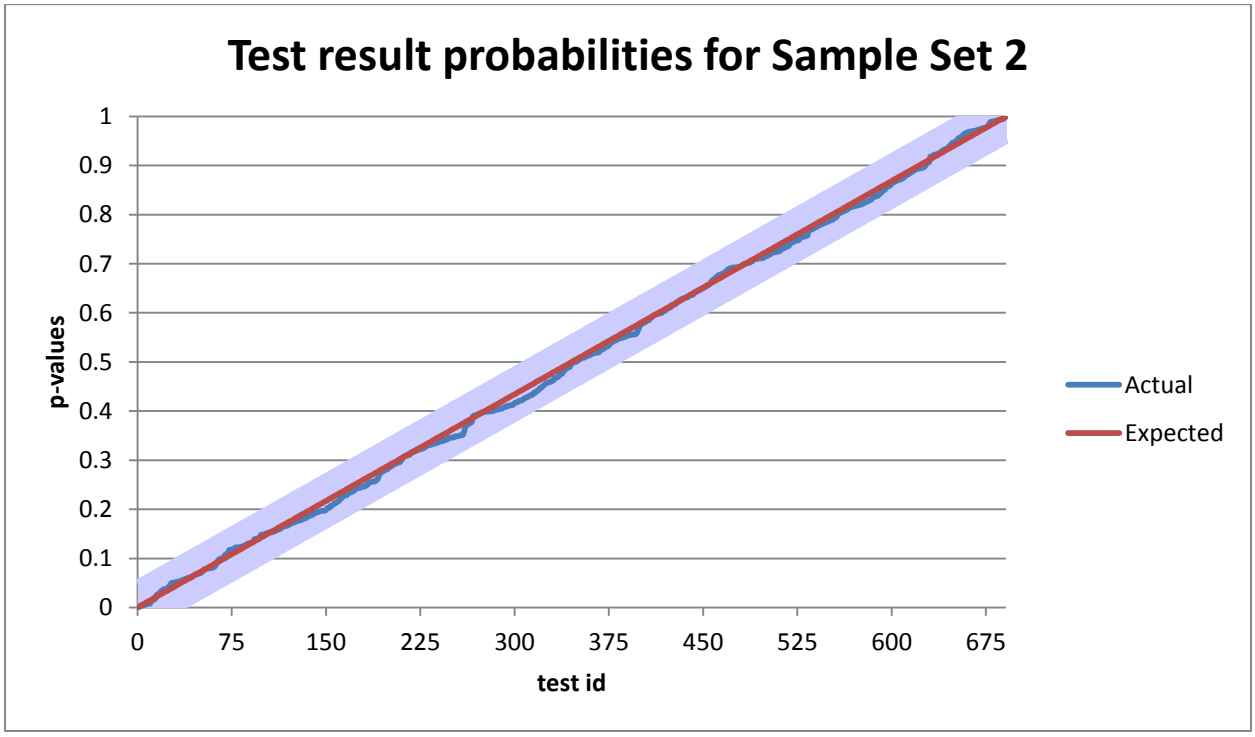

Figure 2: Distribution of result probabilities of tests on sample set 2

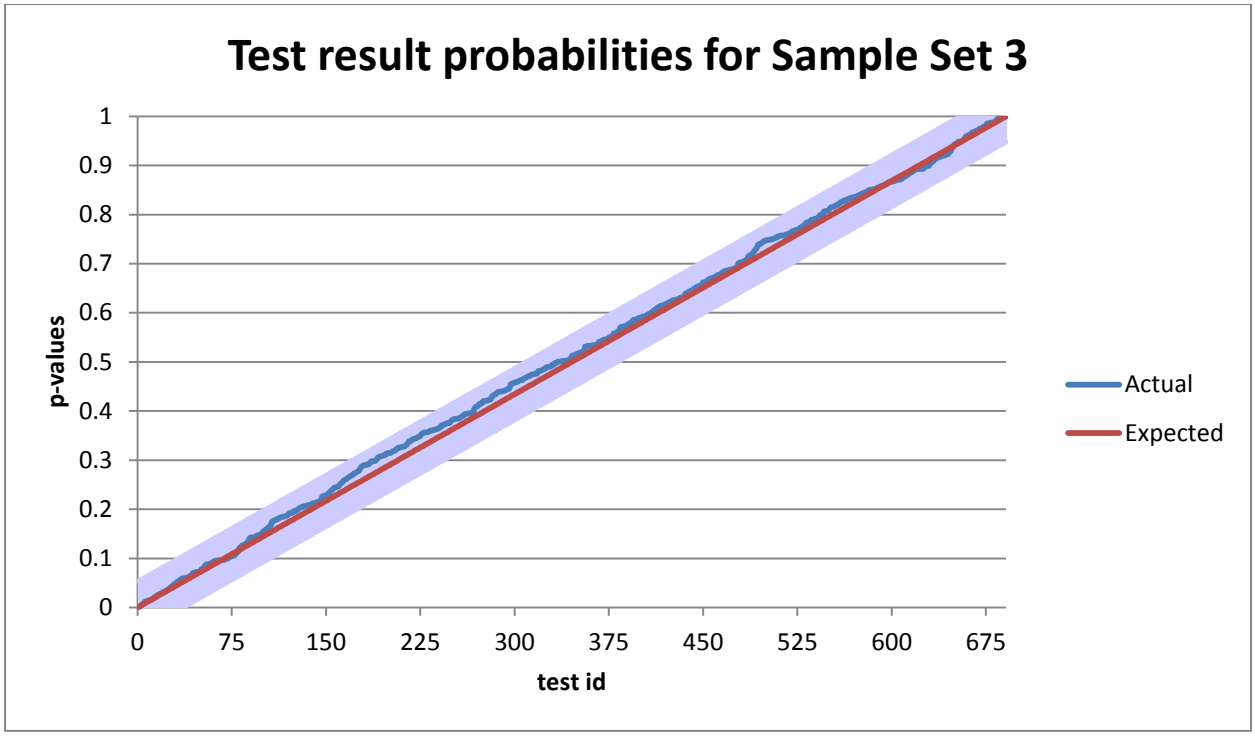

Figure 3: Distribution of result probabilities of tests on sample set 3

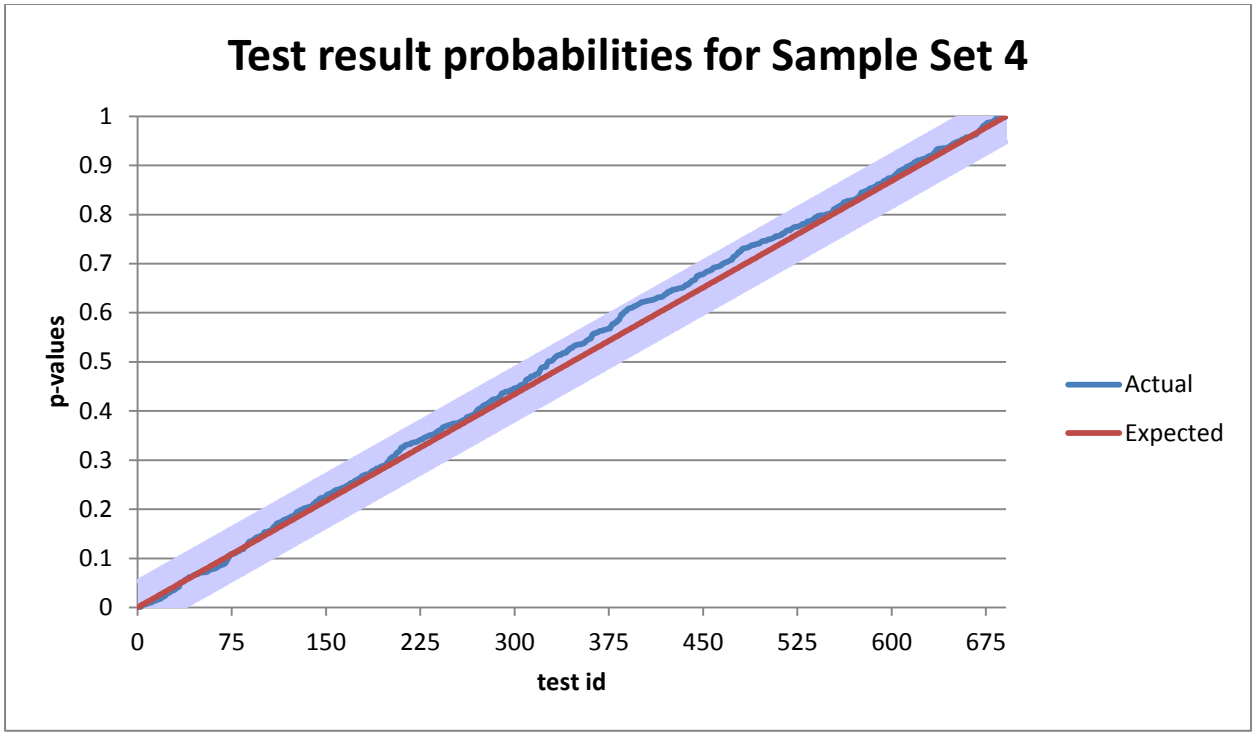

Figure 4: Distribution of result probabilities of tests on sample set 4

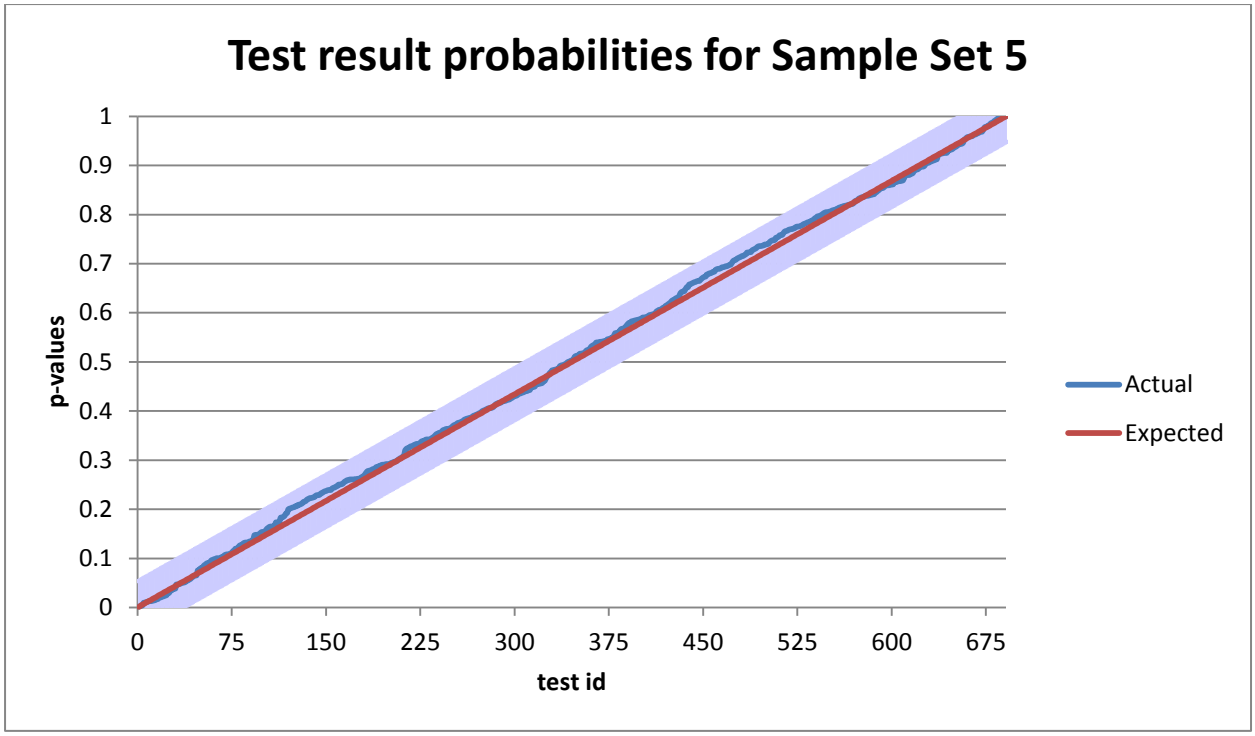

Figure 5: Distribution of result probabilities of tests on sample set 5

5 SOURCE FILES

The relevant source code for the RNG is in the following file:

File Name	SHA-1
HardwareGenerator.cs	B12D0D300B00AAA52A9C9A48A88204E44EA85FBF

6 CONCLUSION

As a result of statistical testing and source code review, BMM believes that the RNG used in Online Gaming provides uniformly random data suitable for its intended application. This RNG complies with the applicable requirements of the GLI-19: Interactive Gaming Systems Version 2.0.