Exploring Quantum Systems for Pseudo-Random Number Generation

Luis Jose Mantilla Santa Cruz[1,a], **Luis F. Faina**[1,b], and **Joao Henrique de Souza Pereira**[1,c]

[1]Federal University of Uberlandia, Faculty of Computing, Uberl andia, Minas Gerais, Brazil
[a]*luis.santa@ufu.br*
[b]*luisfaina@ufu.br*
[c]*joaohs@ufu.br*

Abstract

Quantum realizations have opened a new ways for computer science. The new characteristics and phenomenons allow us to create new algorithms for general proposes. An interesting topic is random number generation. There are two perspectives for this proposes. True random numbers generator (TRN) and pseudo random numbers generator (PRNG). True Random Number Generators has four significant characteristics: randomness, long Period, insensitivity to seeds, repeatability. Additionally, Pseudo Random Number Generators is a fascinating topic that leverages the principles of computer science to craft deterministic algorithms, enabling the creation of a sequence of pseudo-random numbers. A crucial element in this process is the 'seed', which serves as the initial value to generate the entire sequence. This document proposes a algorithm based on a quantum system and the quasi-probability of its possible states to generate a long set of numbers which has pseudo random properties. The quantum system is compound by n qubits, its initial conditions and a small set of rotation gates with a fixed angle. The tests were realized using the battery test called NIST SP800-22, and $\alpha = 0.01$ as a threshold to ensures 99results demonstrate that it is possible generate a long set of pseudo numbers with random characteristics using a quantum simple operation. However, the experiments reveal that a real world implementation require a quantum system with at least 10-9 precision order.

Introduction

Quantum technology offers several new features and has opened the door to a new era - the quantum age. This age began in the early 1980s, when Benioff and Feynman introduced the concept of quantum computing, the main consequencce of the use of quantum mechanism for this propose is the creation of a more effective computer. This theoretical machine is based on qubits as the minimum information unit. Additionally, it has the ability of work with an exponential number of states and realize bast calculations in short time. This new characteristics and phenomenons makes possible the quantum supremacy.

A quantum system is compound by a set of qubits, its initial parameters and the gates destinated to realize changes the qubits. The first component is the qubit which has the property of being in a linear combination of its single states, it means $| \psi> = \alpha \mid 0> + \beta \mid 1\rangle$, where it's complex components have the restriction $\| \alpha \|^2 + \| \beta \|^2 = 1$. An additional consequence is that each auditioned qubit increment exponentially the number of possible states of the system. The second component is the unitary operator which is compound of quantum gates. It allows us to explore the Hilbert's space by making changes into the qubits. The third component is the measurement that makes the system collapse. However, quantum computing requires a change of paradigm for including new quantum phenomenons as part of regular algorithms to develop the counter part of traditional ones.

As consequence of the realization of quantum computers, some new computer science areas were created: quantum communications, quantum computing, quantum sensing, and quantum simulation.

Quantum computing aims to create a counterpart of traditional computing and incorporate new properties such as superposition, entanglement, squeezing, and coherence into algorithms. Some important subareas include quantum circuits and software, quantum hardware, quantum machine learning, and quantum information science. Some of these new methods, techniques, and algorithms are being used to solve real-world optimization problems4–6.

Quantum communication focuses on the development of a new generation of functional communication networks and quantum information study the capacity of the quantum systems to express information, its associated mechanism, and its security. To achieve this goal, researchers deal with quantum entanglement, quantum teleportation, necessary quantum hardware, methods to improve network efficiency, quantum information, quantum cryptography, post quantum cryptography and other related issues.

Random numbers has importance for our lives because many of the real world applications which are used every day requires of it. The definition of generated numbers has four important properties i) Randomness, ii) Long-period, iii) Insensitive 1 to seeds, iv) Repeatability. In addition, many relevant events which have had an impact in economy, human right and others have occurred because the random systems were broken7.

There exists two categories to generate random numbers. First, True-Random Number Generator (TRNG) which uses physical sources of true randomness to generate random numbers. Second, Pseudo-Random Number Generator (PRNG) which uses a deterministic algorithm to generate a set of numbers.

TRNGs operate on the principle that certain physical phenomena, such as electronic noise, radioactive decay, or chaotic systems, are fundamentally unpredictable. These devices capture and convert these naturally occurring processes into random numbers. As a result, TRNGs provide numbers that are statistically independent and uniformly distributed, making them suitable for applications requiring the highest level of randomness and security.

The key advantage of TRNGs is their resistance to predictability, ensuring that the generated numbers cannot be determined, even with complete knowledge of the generator's internal state. This characteristic makes TRNGs invaluable in fields such as cryptography, secure communications, and gambling, where true randomness is essential to prevent exploitation or predictability. However, TRNGs may have limitations in terms of speed and efficiency due to their reliance on physical processes. Despite these limitations, they remain the preferred choice for applications where uncompromising randomness is paramount.

Conversely, a Pseudo Random Number Generators (PRNGs) are a class of algorithms used to generate sequences of numbers that appear random but are, in fact, generated deterministically. These generators rely on initial values, called seeds, and a series of mathematical operations to produce a sequence of numbers that exhibit statistical properties resembling those of truly random sequences. While PRNGs can appear random, they are fundamentally driven by algorithms and initial seed values, meaning that their entropy evolves according to a predictable path.

PRNGs are widely employed in various applications, including simulations, computer graphics, and statistical modeling. They offer several advantages, such as speed and repeatability, as the same seed will always produce the same sequence. This predictability can be beneficial in applications where reproducibility is desired.

Some traditional algorithms were proposed: Yarrow 160, Fortuna, Blum Blum Shub, Counter-Based8. Some new algorithms for criptography based on quantum algorithms was proposed. The most common algorithm modify for this propose is quantum walks9–14. Additionally, new devices based on quantum technology such as QRNG JUR017 was presented and commercialized.

The main limitation of PRNGs lies in their deterministic nature. Given the same initial seed, a PRNG will always produce the same sequence, which makes them unsuitable for applications requiring true randomness and security against predictability. Moreover, PRNGs can exhibit periodicity, where the sequence repeats after a certain number of values.

This document is structured into several key sections. It begins with an introductory exploration of quantum computing. Subsequently, the Results section provides a summary of the theoretical analysis of the probabilities generated by a quantum system, along with the associated statistical tests. The subsequent section is dedicated to the discussion, where the obtained results are analyzed in comparison with JUR01, including discussions on advantages, disadvantages, and the analysis of the nature of the a non-uniform probability distribution by $\triangle H'(A)$. The following section is the conclusion, summarizing the main points. Finally, the document introduces and details the Quantum Quasi-Probability Pseudo Random Generator (QQ-PRG) algorithm for generating pseudo-random numbers.

Results

Generation of long set of numbers pseudo random numbers

The method for generating an extensive list of numbers is analogous to other methods. It is grounded in the resultant quasi-probabilities of the states in a quantum system and a loop which makes possible to obtain a long list of numbers.

To generate a sequence of numbers with random characteristics, a quantum system is initialized, and a sequence of quantum gates is applied sequentially to manipulate the quasi-probabilities of the quantum states. To obtain the pseudo random number, the first $n \geq 6$ most significant elements of the resulting probabilities for each state are discarded, and the next $k > 3$ precision elements are selected as the random number. Each generated number is then appended to the list of numbers.

This method presents an strong dependence on the initial configuration of the quantum system, the initial parameters 'seed', and the set of sequential gates. It dependence also compromise the security of the method due it is necessary know this three parameters to get all the numbers sequence.

This method uses a quantum system to obtain its quasi-probability, its main advantage is given by the number of possible quantum states. The first restriction for the method is related to the quasi probability precision due it must be at least 10^{-9}. The second restriction is given by the number of possible states and it's quasi-probability due as more qubits are included into the system more divided is the information into the states. This phenomenon makes possible the occurrence of states with close to 0 probability.

Probability distribution analysis

In this subsection presents an analysis of two possibilities for probability distribution. First a uniform probability distribution which describe a true random number generator. Second a non-uniform probability distribution which describe the probability into a pseudo random number generator.

Uniform Quantum Probability Distribution with Hadamard Gate

In this context, the quantum probability distribution is divided uniformly into 2 n quantum states, ensuring that $\sum_{i=1}^{2^n} P(a_i) = 1$. This equal division of probability can be likened to complete uncertainty within the quantum system, where each possibility holds equal likelihood, akin to a pure random system.

Quantum computers achieve this uniform distribution by utilizing a fundamental quantum gate known as the Hadamard gate. The Hadamard gate demonstrates its ability to generate a 50% chance of measuring the quantum state $|0\rangle$ and an equally 50% chance of measuring $|1\rangle$. This property serves as the foundation for the proposal put forth in a study by Kumar et al.15. The document establishes that leveraging multiple Hadamard gates can lead to the creation of random sequences of numbers.

This approach illustrates the potential for a True Random Number Generator (TRNG) to be realized using a quantum computer. By harnessing the inherent unpredictability of quantum systems, this method paves the way for applications demanding the highest level of randomness and security, such as in cryptography and secure communications.

Additionally, Shannon's entropy serves as a metric to quantify the uncertainty or randomness inherent in a probability distribution16. In the context of a uniform quantum probability distribution, entropy is defined as

$$H(A) = H(P(a_1), P(a_2)), ..., P(a_{2^n})) = -\sum_i P(a_i) \log_2 P(a_i) \tag{1}$$

In the case of a truly random process, the probability values are identical for every element, indicating maximal uncertainty. Therefore, for a quantum system, we have $H(A) \equiv H(P(a_1)) = H(P(a_2)) = ... = H(P(a_{2^n}))$.

A uniform distribution within a quantum system, consisting of 2n elements observed over N shots, can be represented as

$$H(A) = \sum_{i=1}^{2^n} H(\frac{1}{2^n}) \tag{2}$$

where $P(a_i) = \frac{1}{2^n}, i = 1, ..., 2^n$. This representation is utilized throughout the document, with some modifications and constraints to effectively depict non-uniform probability distributions.

Table 1 provides estimates for a uniformly distributed probability process within a quantum system. Notably, this perspective emphasizes that the introduction of extra qubits into the system leads to a partitioning of the total probability among an expanding set of states. It is essential to recognize that the uniform distribution not only divides the probability but also signifies that the system achieves maximum entropy. This maximum entropy is equivalent to the number of potential states within a quantum system, as demonstrated in Equation 6.

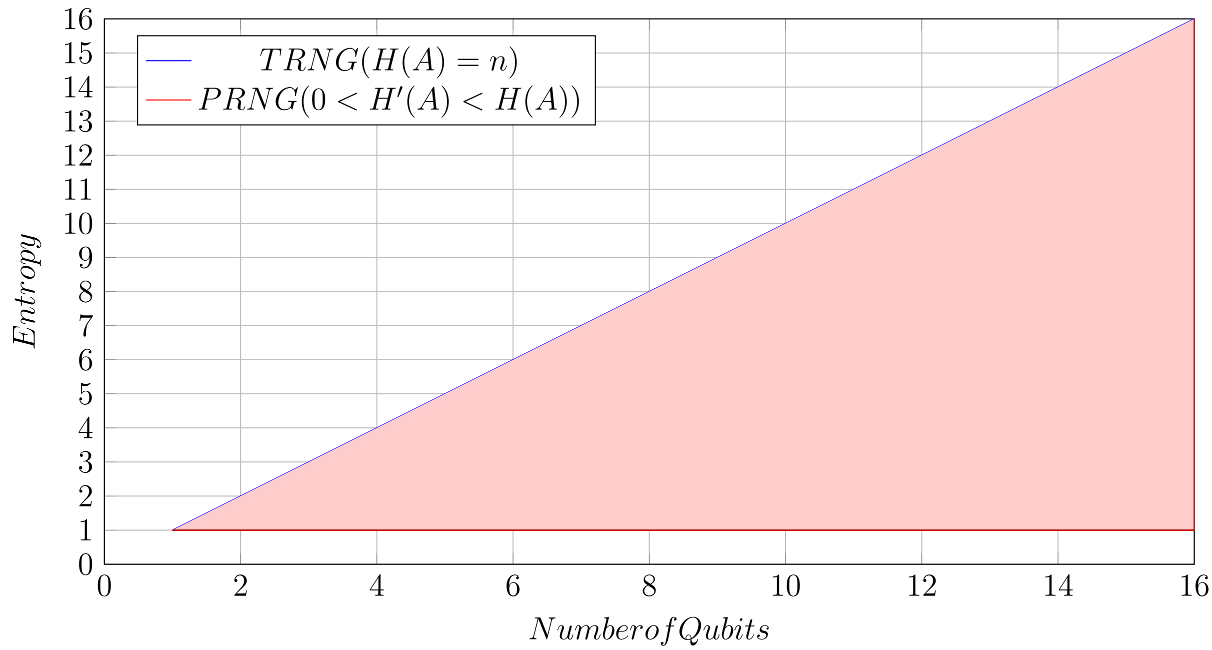


Figure 1: This figure illustrates the entropy of True Random Number Generators (TRNGs) and Pseudo Random Number Generators (PRNGs) in a quantum system with varying numbers of qubits. The blue curve represents TRNGs with H(A) = n, while the red area corresponds to PRNGs with $0 < H'(A) < H(A)$.

Qubits	Possible States	Probability	Shannon's Entropy
1	2	0.5000	1
2	4	0.5000	2
3	8	0.3750	3
4	16	0.2500	4
5	32	0.1563	5

Table 1. Estimates for qubit numbers, possible states, mean probability, and corresponding Shannon's entropy in a random system.

Furthermore, Figure 1 provides a visual representation of the previously computed data. This visualization illustrates the two primary approaches to random number generation. The blue line depicts the entropy for a true random generator based on a specific number of qubits. In contrast, the red area represents the potential entropy achievable by a pseudo-random number generator within a quantum system. This straightforward visualization serves as compelling evidence of the extensive array of possibilities for developing PRNGs based on quantum technology.

Uniform Quantum Probability Distribution with Hadamard Gate

It's essential to understand that probability is distributed among the states of a quantum system. Non-uniform probability distributions can be created within a quantum system through the application of quantum gates. This means that the probability associated with each state can vary, being either less or more than the mean probability.

A representation for a non-uniform distribution can be expressed as:

$$1 = \sum_{i=1}^{2^n} \frac{w_i}{2^n} \tag{3}$$

where $wi \geq 0$. In the case of a uniform distribution, all values of w_i are set to

The entropy of a non-uniform quantum probability distribution is defined as:1

$$H'(A) = H(\frac{w_1}{2^n}, \frac{w_2}{2^n}, ..., \frac{w_{2^n}}{2^n}) = \sum_{i=1}^{2^n} -\frac{w_i}{2^n} \log_2 \frac{w_i}{2^n} \tag{4}$$

where the primary constraint is given by $\sum_{i=1}^{2^n} \frac{w_i}{2^n}$ Moreover, for the proposed approach, it is crucial to quantify the deviation of a non-uniform distribution, denoted as $\triangle H'(A)$, in comparison to the uniform distribution H(A). Both quantum systems consist of the same number of qubits and states, but the latter incorporates variations in probability due to the application of a set of quantum gates.

$$\triangle H'(A) = H(A) - H'(A). \tag{5}$$

The entropy for a uniform distribution (6) is given by:

$$H(A) = -2^n \log_2(\frac{1}{2^n}). \tag{6}$$

The entropy for a non-uniform distribution under the restriction $\sum_{i=1}^{2^n} \frac{w_i}{2^n}$ is expressed as:

$$H'(A) = \sum_{i=1}^{2^n} -\frac{w_i}{2^n} \log_2(\frac{w_i}{2^n}). \tag{7}$$

Further simplification:

$$H'(A) = (n) \sum_{i=1}^{2^n} \frac{w_i}{2^n} - \sum_{i=1}^{2^n} \frac{w_i}{2^n} log_2(w_i). \tag{8}$$

Simplifying this expression:

$$H'(A) = n - \sum_{i=1}^{2^n} \frac{w_i}{2^n} log_2(w_i). \tag{9}$$

Finally, the deviation of H'(A) in relation to H(A) is defined as:

$$\triangle H'(A) = \sum_{i=1}^{2^n} \frac{w_i log_2(w_i)}{2^n}. \tag{10}$$

The deviation concerning a uniformly distributed probability provides us with the following insights:

- The maximum entropy achieved by a uniform distribution, denoted as $H(A)$, is equal to the number of elements in the quantum system, n.

- The only case where $\triangle H'(A) = 0$ is the trivial scenario in which $w_i = 1, i = 1, ..., 2^n$. In non-trivial cases where $w_i \neq 1, i = 1, ..., 2^n$,it follows that $0 \leq H(A) < H(A)$.
- The value of $\triangle H'(A)$ varies in proportion to the deviation of each w_i i from unity. The smaller the deviation, the closer the value of $\triangle H'(A)$ is to $H(A)$.

Statistical test

In this subsection, the generated sequence of numbers with random properties, obtained through the innovative quantum circuit construction, is subjected to rigorous statistical testing using the NIST SP 800-22 suite. Comprising 15 distinct tests, each designed to calculate various indices for the provided binary data, these evaluations are crucial to determining the randomness and reliability of the generated sequence. For each of the 15 tests, a predefined threshold value $\alpha = 0.01$ is established, signifying that the generated sequence must exhibit a 99% probability of being genuinely random to pass the test. The sequence under examination consists of a vast array of 4,194,304 decimal numbers. Each decimal number, comprised of three digits falling within the range of [0,999], is represented as a 10-bit string. In consequence, the entire raw dataset comprises a sequence of 41,943,040 binary digits, obtained from the execution of 524,288 quantum circuits. Each circuit was composed of 3 qubits, utilized a scaling factor of f s $= 1/100$, employed a uniform set of rotation gates for each axis, and set rotation angles at $\frac{\pi}{2} \times 0.19$ for each rotation gate. The evaluation of the statistical properties of the generated sequence, a fundamental aspect of this study, is visually represented in Figure 2. The figure illustrates that the generated numbers exhibit a tendency to follow a uniform distribution within the interval [0,999]. Rigorous statistical tests, conducted using the NIST SP 800-22 suite, offer valuable insights into the robustness and authenticity of the quantum-generated random numbers. These tests serve to ensure the practical applicability of the generated random numbers in various real-world scenarios.

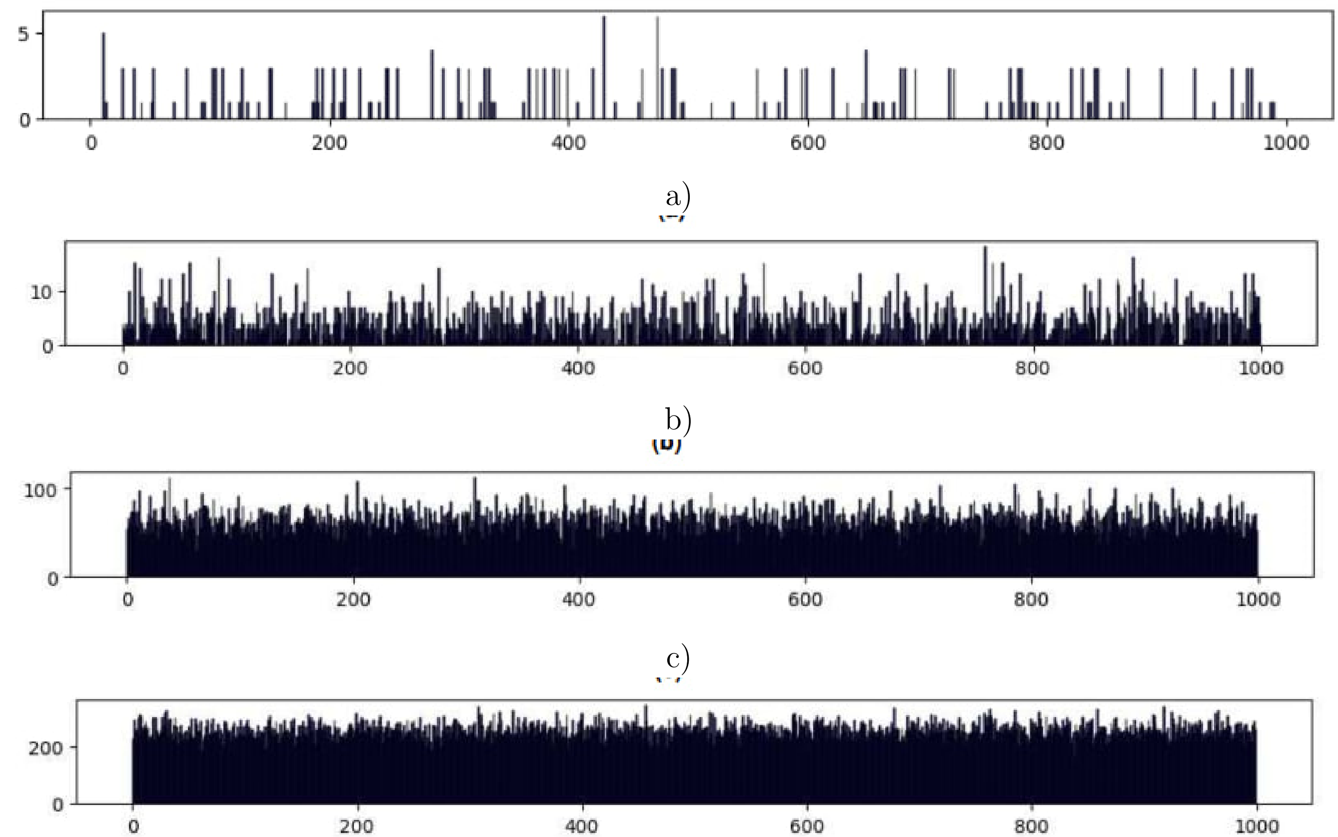
Equipment Description

The generation and evaluation of random sequences were facilitated by cutting-edge quantum computing tools, notably the Aer Simulator and the IBM Qiskit framework. The Aer Simulator served as a foundational element, providing a versatile and efficient platform for simulating quantum circuits. Additionally, IBM Qiskit, a comprehensive open-source quantum computing framework, formed the backbone of our experimentation.

Discussion

The proposed quantum random number generation approach leverages the superposition of qubits within a quantum system. After performing N measurements, we obtain the corresponding quasi-probabilities for specific configurations, allowing us to generate 2^n quasi-probabilities corresponding to the possible states of the quantum system.

The main advantages of this approach can be summarized in its simplicity. It requires a small number of qubits, an initial configuration, and a set of quantum gates that sequentially rotate the qubits. This deterministic mechanism enables the generation of a specific set of numbers dependent on the initial configuration. This algorithm has demonstrated its capability to generate a long sequence of numbers with random properties. The terms wi in the sequence are subject to the constraint n =



a)

b)

c)

d)

Figure 2: Visualizing the Distribution of Incremental Number Sequences through Histograms: a) The first 256 numbers. b) The initial 4096 numbers. c) The opening 65536 numbers. d) The foremost 262144 numbers..

1. This constraint significantly impacts the sequence of number generation as these terms determine the entropy of a non-uniform distribution. Moreover, these terms serve as a measure to evaluate the similarity of a distribution to a uniform distribution. One of the main advantages of the proposal is its efficiency in generating a long sequence of numbers. This is achieved through the periodicity of the deterministic algorithm and the methodology used to represent numbers with significant digits ranging from 10-6 to 10-9 as binary strings or numbers in the binary system. However, a limitation of the proposal is its inability to scale the number of used qubits. This limitation arises because the number of possible states increases exponentially with the number of qubits, affecting the probability distribution of states. A quantum system that generates a uniform probability distribution divides the probability evenly among 2 n states. In contrast, a non-uniform distribution can be represented by modifying a uniform probability through a set of terms wi , while still satisfying the constraint n = 1. This alteration can result in significant digits between 10-6 and 10-9 being set to zero, requiring the algorithm to find numbers with even smaller significant digits and increasing the number of measurements to improve precision. The equation is of particular interest in this proposal. This term accommodates values of wi within the range , allowing for a wide range of distributions. The trivial case is when wi = 1, i = 1,...,2 , which permits an infinite variety of distributions of the values wi . This equation has been the subject of study by various researchers17, 18 and possesses intriguing properties. Notably, the more wi deviates from unity, the more the resulting entropy deviates from the maximum entropy, opening the door to novel insights for measuring the proximity of a distribution to the maximum entropy in a quantum system. The results obtained from the application of the NIST SP800-22 test battery are presented in Table 2. These results

C1	C2	C3	Shannon's STATISTICAL TEST
1	2	0.5000	112312
2	4	0.5000	231231
3	8	0.3750	3123123
4	16	0.2500	412312
5	32	0.1563	512313
5	32	0.1563	512313
5	32	0.1563	51231
5	32	0.1563	53123
5	32	0.1563	51231
5	32	0.1563	51231
5	32	0.1563	56785
5	32	0.1563	58678
5	32	0.1563	56456
5	32	0.1563	532452
5	32	0.1563	556246
5	32	0.1563	5262
5	32	0.1563	523423

Table 2. Estimates for qubit numbers, possible states, mean probability, and corresponding Shannon's entropy in a random system.

demonstrate success in 3 out of the 15 tests. To provide context, the results are compared with those of a real-world quantum random number generator named JUR01, and this comparison is presented in Table 3. Both generators employ different methodologies for generating sets of numbers, each with its own advantages. The primary advantage of the proposed approach is its capability to pass a universal test. However, a notable limitation is the absence of an adequate methodology to rotate the qubits to generate a non-uniform probability distribution that closely approaches the maximum entropy.

Conclusion

In summary, the proposed quantum algorithm demonstrates a novel approach to random number generation by exploiting the superposition of qubits within a quantum system. It offers a range of advantages, including simplicity, efficiency, and the ability to control entropy in the generated numbers. However, it comes with certain limitations, primarily related to its scalability and the need for improved methods to achieve non-uniform distributions close to maximum entropy. The algorithm's success in passing a significant portion of the NIST SP800-22 tests is a noteworthy accomplishment, highlighting its potential in providing random numbers for various applications. Its unique exploration of entropy variations, especially in measuring a distribution's proximity to maximum entropy in a quantum system, presents promising prospects for further research. As the field of quantum computing continues to evolve, addressing the algorithm's limitations and refining its methodology for generating non-uniform distributions could unlock a wealth of opportunities across multiple domains. This work signifies a significant step in the direction of deterministic quantum algorithms, offering a long periodicity that can excel in random testing. Future developments in this area hold the promise of generating high-quality random numbers and advancing quantum computing applications.