Quantum Random Number Generation via Von Neumann Projection

Nawres A. Alwan[1], Suzan J. Obaiys[1(✉)], Nadia M. G. Al-Saidi[2], and Nurul Fazmidar Binti Mohd Noor[1]

[1] Department of Computer System and Technology, Faculty of Computer Science and Information Technology, Universiti Malaya, 50603 Kuala Lumpur, Malaysia
s2000740@siswa.um.edu.my, {suzan,fazmidar}@um.edu.my
[2] Department of Applied Sciences, University of Technology, Baghdad 10066, Iraq
nadia.m.ghanim@uotechnology.edu.iq

Abstract. This work introduces a new method for quantum random number generation (QRNG) based on a new model of n-dimensional quantum hyperchaotic systems (nD−QHCS) called nD Quantum Hyperchaotic Random Numbers Generation (nD-QHCRNG), which is derived from the classical n-dimensional hyperchaotic systems (nD-HCS) [1]. Our approach leveraging quantum measurement uncertainty via Von Neumann (VNman) projection to produce truly random bit sequences of nD-QHCS. The quantum system is described by the Hamiltonian $\hat{H} = \sum_{i=1}^{n} \frac{\hat{p}_i^2}{2} + \sum_{i=1}^{n} (A\hat{q}_{i+1}\hat{q}_{i-1} - B\hat{q}_{i-2}\hat{q}_{i-1})$ with $\hat{p}_i = -i\hbar\frac{\partial}{\partial q_i}$, where $\hat{p}_i$ and q_i are the momentum and position of quantum system, respectively. The system exhibits complex quantum dynamics behavior with substantial entanglement between degrees of freedom. The proposed method harnesses quantum randomness through the measurement process, where the system evolves under the hyperchaotic Hamiltonian, quantum measurements induce wavefunction collapse according to the VNman projection axiom, and thus generate nondeterministic outcomes. Statistical analysis of bit sequences produced by the nD-QHCS generator demonstrates exceptional randomness quality, passing all NIST tests successfully. The nD-QHCS method combines the sensitivity to initial conditions characteristic of classical nD-HCS with the fundamental indeterminism of quantum measurement, resulting in a QRNG with entropy values approaching theoretical maximums. The performance analysis shows negligible autocorrelation and uniform distribution of bit patterns, making this method suitable for cryptographic applications requiring high-quality randomness.

Keywords: Quantum random number generation · Von Neumann projection · Hyperchaotic · Hamiltonian · quantum hyperchaotic system

1 Introduction

Quantum physics is a crucial field in many applications. It has recently been utilized to generate random numbers that have vital roles in cryptography,

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
O. Gervasi et al. (Eds.): ICCSA 2025, LNCS 15648, pp. 176–193, 2025.
https://doi.org/10.1007/978-3-031-97000-9_11

such as generating crypto codes or concealing messages. The following procedure was created by J. Von Neumann (VNman) in 1946 as a pseudo-random generator (PRNG): "start with an initial random seed value, square it, and slice out the middle digits." Some statistical characteristics of randomness are present in a sequence that is produced by applying this procedure repeatedly. Although PRNGs are entirely determined by the seeds, electronic network traffic is encrypted every day using hundreds of billions of pseudo-random numbers. In the age of the internet, their weaknesses have been identified. As an illustration, consider the 2012 discovery of a problem in the RSA encryption technology, which was linked to the numbers generated by a PRNG [2]. Quantum random number generators (QRNGs) have been developed over decades and experimented with using many different quantum sources. These sources are mainly based on single photons, laser phase fluctuation, vacuum states, and path-entangled quantum states. However, imperfection in QRNG systems results in deviation from the ideal models used in security analysis, which can lead to the risk of side information leakage, making the produced random numbers predictable [3]. To address these shortcomings, several kinds of random generators, specifically, quantum random number generators (QRNGs), have been created. Because greater quality randomness is needed in many fields, including physics [4,5], medicine [6], statistics [7], information science [8], and cryptography [9], QRNGs have become more and more popular in the past ten years. Also, QRNGs are predicated on the "fundamental unpredictability of well-chosen and controlled quantum processes," [10] they are regarded as "better than PRNGs". We can see this claim is weak, especially as it is widely recognised that the concept of "true randomness," which is understood to mean "lack of correlations" or "maximal randomness," is mathematically meaningless [11]. Is it possible for QRNGs to be "provably better" than PRNGs? Two categories of "theoretically certified" QRNGs exist: those based on the Bell inequalities [12,13] as well as by the Located Kochen-Specker Theorem [14], which is a variant of the Kochen-Specker Theorem (see 10-12). For more details, see [15]. Several methods are introduced to generate random numbers (GRN) (classical, quantum). In classical models, authors study many methods for GRN, such as [16,17] or quantum [18,19]. In this study, we present a new quantum random number generation (QRNG) framework based on n-dimensional quantum hyperchaotic systems (nD-QHCS). Our approach begins with transforming a classical n-dimensional hyperchaotic system (nD-HCS) [1] with Hamiltonian into its quantum counterpart through canonical quantization, resulting quantum Hamiltonian $\hat{H}$. This quantum system preserves the classical chaotic properties while introducing fundamental quantum uncertainty. The quantum state evolves according to the Schrödinger equation, leveraging hyperchaotic dynamics with multiple positive Lyapunov exponents to ensure extreme sensitivity to initial conditions. The core innovation lies in our application of VNman projection to extract randomness: The initial Gaussion wavepacket $|\psi_0\rangle$ is prepared, evolve it under the hyperchaotic Hamiltonian, perform measurements on either position or momentum observables, causing the state to collapse according to $|\psi\rangle \to |\psi'\rangle = \frac{P_i|\psi\rangle}{\sqrt{\langle\psi|P_i|\psi\rangle}}$

and extract random values from the measurement results. This process guarantees randomness from both quantum measurement uncertainty and chaotic dynamics, creating a dual layer of unpredictability. Statistical analysis demonstrates that our system successfully passes all NIST SP 800-22 tests, exhibiting higher entropy rates, lower autocorrelation, improved environmental resistance, and enhanced security compared to existing QRNG approaches. The dimensional scaling properties of our system allow for performance optimization by increasing the system dimension, while tunable coupling parameters A and B enable customization for specific applications ranging from cryptography to scientific modeling and AI. Our nD-QHCRNG thus represents a significant advancement in QRNG technology, combining theoretical rigor with practical implementation pathways for modern quantum computing platforms. Unlike previous traditional QRNG approaches such as photon-based or vacuum-fluctuation methods [2,20], the previous quantum random number generation (QRNG) methods primarily relied on single photons or basic quantum effects, which often suffer from predictable biases or environmental vulnerabilities. In contrast, this work introduced a new nD-QHCRNG integrated with VNman projection, providing unpredictability and significantly reducing bias compared to earlier models. Also, in our work, we utilized Python 3.11 [21] language to help us with some analysis, plots of figures, and to implement the quantum circuit for the nD-QHCRNG via the qiskit library.
The main aspects of this paper are as follow:

1. Built a new model of QRNG based on nD-QHCS.
2. Utilizes Heisenberg's uncertainty principle to measure the quantum state and induce wavefunction collapse through the VNman projection, thereby achieving true randomness.
3. Our model of QRNG demonstrates high randomness quality verified through comprehensive statistical tests, including NIST, entropy analysis, and autocorrelation
4. Offers improved randomness characteristics with low autocorrelation, negligible bias, and entropy near the theoretical maximum, making it suitable for secure cryptographic applications.

The remainder of this work is structured as follows: Sect. 2 introduces the nomenclature and definitions of key concepts in quantum mechanics. In Sect. 3, we present our proposed method for generating nD-QHCRNG based on the VNman projection. Section 4 provides statistical analysis using various tests, including NIST, entropy, and autocorrelation tests. Section 5 offers a discussion of the results, and Sect. 6 concludes the paper.

2 Nomenclature and Definitions

2.1 Quantum Mechanical and Von Neumann (VNman) Projection

A vector $|\psi\rangle$ in quantum state is called "ket psi" in a complex Hilbert space $\mathcal{H}$, a complete vector space equipped with an inner product. At the same time the

dual vector $\langle\psi|$ called "bra psi" belongs to the dual space $\mathcal{H}^*$. Whereas, the inner product $\langle\varphi \mid \psi\rangle$ represents the probability amplitude between states $|\varphi\rangle$ and $|\psi\rangle$ or called (eigenvalues). The probability of measuring state $|\varphi\rangle$ is $|\langle\varphi \mid \psi\rangle|^2$ when the system is in state $|\psi\rangle$. Quantum observables are represented by Hermitian operators $\hat{A}$ acting on the Hilbert space, with eigenvalues a_i corresponding to possible measurement outcomes and eigenvectors $|a_i\rangle$ representing the system state after measurement. The expectation value of an observable $\hat{A}$ in state $|\psi\rangle$ is given by $\langle\hat{A}\rangle = \langle\psi|\hat{A}|\psi\rangle$. The position operator $\hat{q}$ and momentum operator $\hat{p} = -\frac{i\hbar\partial}{\partial q}$ satisfy the commutation relation $[\hat{q}, \hat{p}] = i\hbar$, forming the foundation of quantum uncertainty [22]. VNman projection measurement describes the instantaneous change of a quantum state upon measurement. When measuring an observable $\hat{A}$ with eigenstates $|a_i\rangle$, the state $|\psi\rangle$ collapses to $|a_i\rangle$ with probability $P(a_i) = |\langle a_i \mid \psi\rangle|^2$. Mathematically, this projection is represented by the action of the projection operator $\hat{P}_i = |a_i\rangle\langle a_i|$ on the quantum state: $|\psi\rangle \rightarrow |\psi'\rangle = \widehat{P}_i|\psi\rangle / \sqrt{\langle\psi|\widehat{P}_i|\psi\rangle}$ [22].

2.2 Quantum Computing and Random Number Generation

In this section, a brief introduction to quantum computing and random number generation without claiming to be exhaustive. For more in-depth explanations, we refer to the cited literature. Quantum computing leverages quantum mechanical phenomena such as superposition and entanglement to perform calculations that would be infeasible for classical computers. The fundamental unit of quantum information is the qubit, which, unlike classical bits, can exist in superpositions of states. Quantum random number generators exploit the inherent probabilistic nature of quantum mechanics to produce true random numbers, as opposed to the pseudo-random numbers generated by classical algorithms. Traditional QRNGs typically rely on simple quantum systems such as single photons passing through beamsplitters or radioactive decay [3].

2.3 Randomness in Quantum Mechanics

Let's come back to the early 20th century, when quantum mechanics was born. The Copenhagen interpretation was formulated in 1927 [23] in Copenhagen by Niels Bohr and Werner Heisenberg, building on Max Born's idea of interpreting the wave function probabilistically. In this view, the square of the wave function's modulus in the position representation gives the probability density of finding a particle at a particular point in space—this is often referred to as the standard interpretation. However, this interpretation contrasts with Fuchs' approach [24], which advocates a competing probabilistic concept known as Quantum Bayesianism. The measurement of a quantum system in the Copenhagen representation initially realises the superposition of quantum states by choosing at random one of the numerous possible classical states. This choice is due to the so-called collapse of the wave function due to the interaction of an external observer (i.e., an external macroscopic measuring system characterized by a number of degrees

of freedom corresponding to at least the Avogadro number) with the measured quantum system. VNman [22] has conducted research on the quantum measurement technique. As a result, VNman presented a "ansatz", which may be written as an axiom saying that when the measurement takes place, the wave function of the quantum system collapses in a really random fashion into one of the states of the measured observable basis. At each given moment t in time (at which the measurement takes place), this can be defined as:

$$\begin{aligned} \psi(\mathbf{r}, t) &= \sum_i c_i(t)\phi_i(\mathbf{r}), \\ \hat{A}\phi_i &= \lambda_i \phi_i \end{aligned} \tag{1}$$

where λ_i is the eigenvalue of the $\hat{A}$ operator, and $\mathcal{H}$ is a Hilbert space covered by eigenstates of the observable $\hat{A}$ creating the base ϕ_i. The measurement in this formulation consists of choosing one state ϕ_i for which c_i is non-zero in an unpredictable random fashion. In this scenario, the measured quantum system assumes a randomly chosen state ϕ_i, and the macroscopic number of degrees of freedom of the measuring device reflects the eigenvalue λ_i. This enables us to observe the system in the traditional manner as the outcome of a measurement of a specific physical observable that corresponds to $\hat{A}$. Only the odds of various ϕ_i eigenstates of the measured observable occurring as a random consequence of the measurement are defined by the square of the modulus of c_i coefficients. This method makes the assumption that frequency probabilities exist, which presents a serious issue with the way quantum physics is expressed. This method makes the assumption that there are an endless number of identical copies of the system being monitored, and that the coefficients c_i will determine the distribution of certain states in the measurements made on future copies. However, this contradicts the destructive and unique nature of quantum measurement. According to the above-mentioned interpretation, the frequency likelihood of an event occurring in a particular process is defined as the limit of the relative frequency of obtaining such an event in the implementation of an infinite number of such processes.

$$P(x) = \lim_{N \to \infty} \frac{n}{N} \tag{2}$$

where N is the number of process repetitions, and n is the number of process reruns in which the event took place. The difficulty of performing a quantum measurement an infinite number of times is an issue in this context. The idea of a probability paradigm in quantum mechanics was based on this issue. Fuchs uses the weather forecast as an example to explain this issue [24]. Since we are dealing with a circumstance that has never occurred before while predicting the weather for the following day, we are unable to apply the frequency probability paradigm, which is based on occurrences that can be frequently observed. The Bayesian probability paradigm ought to be taken into consideration instead. It is necessary to base the weather forecast on knowledge of comparable but distinct circumstances. As a result, the conditional probability can be used to

determine it. According to Fuchs, the same is true for quantum measurement, which is a special process due to its destructive nature. We refer to this method as quantum Bayesianism [24]. According to quantum Bayesianism, the state of a quantum system can be viewed as either subjective, as indicated by the observer's expectation of the system, or objective, as indicated by the measure of objective probability. The idea of a quantum random number generator may be significantly affected by these distinctions. Therefore, the issue of randomness can also be linked to the interpretation of quantum mechanics itself, which is not clear-cut in this regard, as well as the technological flaws in the application of a particular solution based on quantum physics. An unidentified quantum state, an unidentified coherent superposition of known states, and random decoherence (measurement) all contribute to the quantum aspect's randomness. The preparation of the unknown state and whether it is known to another observer who would be able to speak with a local observer taking a measurement on what he perceives to be an unknown condition are the questions that come up here, though. As a result, it appears that the actual definition of randomness might be derived from the quantum measurement process, but only from true quantum information, making it essentially undefinable as far as any classical observer is concerned. The existence of such information is an open question that presents philosophical epistemological issues. Thus, we can notice the existence of some interesting randomness properties for such information. It turns out that the randomness contained in a single qubit of such unknown information might be equivalent to the randomness contained in any arbitrary number n of qubits and is related to the concept of quantum entanglement [20].

2.4 Quantum Random Numbers

Generating random numbers is of great practical importance in several fields, as it is mentioned in the introduction section; either in the classical state [16,17] or in the quantum state [18,20]. Only pseudorandom bit sequences are produced using the available numeric methods. They can be tested using probability calculus and statistics [25], but it's important to keep in mind that a chosen portion of a pseudorandom sequence may pass randomness tests while still being deterministic in nature. For instance, they are adequate for computer games, but they don't meet the randomness requirements for cryptographic security techniques and accurate mathematical simulations. This circumstance arises from the statistical character of the tests themselves, meaning that the negative result, which rejects the sequence as unquestionably pseudorandom, rather than the good outcome of the tests is what counts. The congruence algorithm (Linear Congruential Generator) is an illustration of a basic pseudorandom number generator: (The known constants a, b, and m have been chosen appropriately): The seed value serves as the beginning state, the output bit is chosen at random, and the subsequent bit is produced using the following formula: new state $= a\tilde{A}-$ old state $+b \bmod (m)$, generated bit = new state $\bmod (2)$ is a call to a cryptographic hash algorithm (like MD5 or SHA1) that is iterative. Some pseudorandom generators are not secure; that is, they produce pseudorandom sequences that lose their

randomness because they can be predicted with a significant enough computational investment. The physical characteristics of the computer itself, such as unpredictable input-output activity intervals, processor temperature variations, or keypad signal frequency, are frequently used to generate pseudorandom sequences using traditional physical pseudorandom number generators. In actuality, the different hardware electrical noise generators that are thought to be genuinely non-deterministic are pseudorandom generators. The analogy of randomness, for instance, can be used for the situation of water vapour bubbles on a boiling water surface. It could be assumed that volumetric boiling, which results in an irregular, dynamic pattern of the boiling water's surface, is random when the water vapour pressure surpasses the hydrostatic pressure due to the microscopic nature of the beginning of the production of closed surface elements (vapour bubbles) inside the liquid. Nonetheless, it is simple to observe that, for instance, by adding a small amount of sand to the water, you can identify the locations where bubbles form, and that the sides of a powerful fan can significantly alter the boiling water's surface appearance. In this way, the so-called bias can be introduced, significantly altering what appears to be random behaviour. This might also resemble a straightforward bias towards tossing a coin with an asymmetrically profiled edge or asymmetrically loaded dice. Disrupting randomness in lengthy sequences may be crucial in these situations, as dishonest tactics, such as in games involving loaded dice, marked cards, or magnetically distorted roulette, readily demonstrate [20].

3 VNman Projection for nD Quantum Hyperchaotic System

In this section, the nD-QHCRNG is introduced based on VNman projection. According to [1], the hyperchaotic system, defined as;

$$\frac{dX_i}{dt} = \left(AX_{i+1} - BX_{i-2}\right) X_{i-1} \tag{3}$$

where X_i are the state variables and A, B are parameters. The first step and based on [18], the classical Hamiltonian system can be defined as

$$H = \sum_{i=1}^{N} \frac{p_i^2}{2} + \sum_{i=1}^{N} \left(Aq_{i+1}q_{i-1} - Bq_{i-2}q_{i-1}\right) \tag{4}$$

where $\sum_{i=1}^{N} \frac{p_i^2}{2}$ is kinetic energy (T) and $\sum_{i=1}^{N} \left(Aq_{i+1}q_{i-1} - Bq_{i-2}q_{i-1}\right)$ is potential energy (V) of H. Based on canonical quantization, the quantum Hamiltonian system is defined as

$$\hat{H} = \sum_{i=1}^{N} \frac{\hat{p}_i^2}{2} + \sum_{i=1}^{N} \left(A\hat{q}_{i+1}\hat{q}_{i-1} - B\hat{q}_{i-2}\hat{q}_{i-1}\right) \tag{5}$$

where $\hat{p}_i = -i\hbar\frac{\partial}{\partial q_i}$ are the momentum operators, then (5) becomes as follow:

$$\hat{H} = \sum_{i=1}^{N} \frac{\hat{p}_i^2}{2} + \sum_{i=1}^{N} (A\hat{q}_{i+1}\hat{q}_{i-1} - B\hat{q}_{i-2}\hat{q}_{i-1}) \tag{6}$$

Figure 1 shows an example of the sensitivity analysis of A and B of nD-QHCS with respect to entropy.

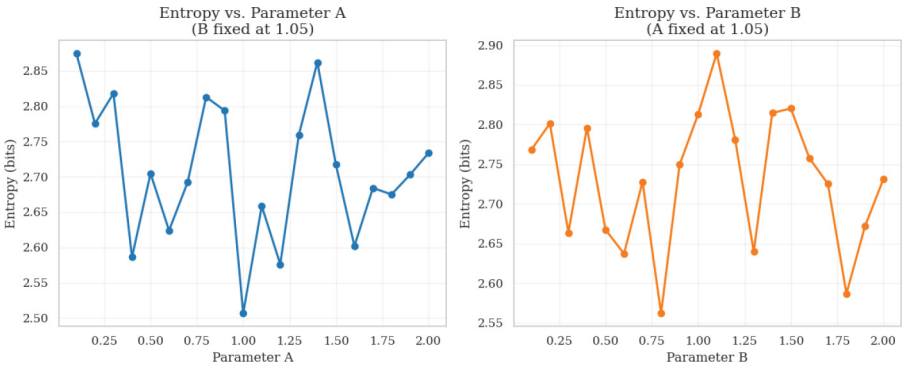


Fig. 1. Sensitivity analysis of A and B of nD-QHCS with respect to entropy.

Before applying VNman projection measurement, we prepare the system in a well-defined initial quantum state, typically a Gaussian wavepacket:

$$|\psi_0\rangle = \frac{1}{(\pi\sigma^2)^{N/4}} \exp\left(-\frac{\sum_{i=1}^{N} q_i^2}{2\sigma^2}\right) \tag{7}$$

where σ controls the width of the wavepacket in position space. This state has a well-defined position and momentum distribution, satisfying the minimum uncertainty relation. The initial state evolves under the hyperchaotic Hamiltonian according to the Schrödinger equation:

$$i\hbar\frac{\partial\psi(\boldsymbol{q},t)}{\partial t} = \hat{H}\psi(\boldsymbol{q},t) \tag{8}$$

Then, the solution has the following mathematical formula:

$$\psi(\boldsymbol{q},t) = \sum_j c_j\phi_j(\boldsymbol{q})e^{-iE_jt/\hbar} \tag{9}$$

where $\phi_j(\boldsymbol{q})$ are the eigenfunctions of $\hat{H}$ with eigenvalues E_j. According to the VNman projection postulate, when we measure an observable $\hat{A}$, which could be position, momentum, or any other observable, yields

1- The measurement will yield an eigenvalue a_k of $\hat{A}$, 2- The probability of obtaining the eigenvalue a_k is $P(a_k) = \sum_j |c_j|^2 |\langle \chi_k \mid \phi_j \rangle|^2$, where χ_k are the eigenfunction of $\hat{A}$ 3- Then, upon measurement, the system state collapses to the following:

$$\psi_{\text{after}}(\boldsymbol{q}) = \frac{\hat{P}_k \psi(\boldsymbol{q}, t)}{\sqrt{\langle \psi(t) | \hat{P}_k | \psi(t) \rangle}} \tag{10}$$

where $\hat{P}_k = |\chi_k\rangle \langle \chi_k|$ is the projection operator. This projection process is fundamentally random according to quantum mechanics, and the hyperchaotic evolution ensures that the probability distribution is: • Highly sensitive to initial conditions • Effectively unpredictable • Uniformly distributed (in the long-term average) The measured eigenvalue λ_j contains quantum randomness that we can extract via four steps:

1. Direct mapping: For position measurements in the range $[-L, L]$:

$$r = \frac{q_i + L}{2\,L} \tag{11}$$

   This maps the position to a random number between 0 and 1.
2. Digital extraction: For high-precision measurements:

$$d = \lfloor (|q_i| + C_1) / C_2 \rfloor \bmod 10 \tag{12}$$

   where C_1 and C_2 are constants chosen to optimize randomness
3. Binary extraction: For generating random bits:

$$b = \begin{cases} 1 & \text{if } q_i > 0 \\ 0 & \text{if } q_i < 0 \end{cases} \tag{13}$$

4. Multiple extractions: From a single measurement of an n-dimensional system, multiple random values can be extracted by measuring different coordinates.

Algorithm 1 illustrates the nD-HCRNG processing.

Figure 2 shows the Quantum circuit of $n\mathrm{D}-\mathrm{QHCRNG}$ where $\mathrm{n} = 100$. Begin with the initial state includes all qubits initialized in the computational basis state $|0\rangle$. Then, multiply each qubit by a Hadamard transformation (H gate) to produce an equal superposition for all possible states. This step is essential for encoding quantum parallelism into the system, enabling the simultaneous evaluation of multiple quantum trajectories across the Hilbert space. After that, each qubit is subjected to an R_z gate, representing phase evolution and incorporating the momentum term $\sum \frac{p_i^2}{2}$ of the Hamiltonian. These rotations are dependent on the specific quantum kinetic energy contribution associated with each qubit. Following this, the circuit applies entangling operations, denoted as items A and B, to encode the nonlinear interaction terms of the nD-quantum Hamiltonian system. The A implement the $Aq_{i+1}q_{i-1}$ interaction, while the B implement the

Algorithm 1. Quantum Random Number Generator

Require: A = coupling parameter for $q_{i+1}q_{i-1}$ term, B = coupling parameter for $q_{i-2}q_{i-1}$ term, N = dimension of hyperchaotic system, $\hbar$ = reduced Planck constant, numRandomNumbers = number of random numbers to generate, evolutionTime = time to evolve system between measurements, σ = initial wavepacket width

Ensure: randomNumbers[] = array of quantum random numbers

procedure ConvertToQuantumSystem(A, B, N)
  $\hat{H} = \sum_{i=1}^{N} \frac{\hat{p}_i^2}{2} + \sum_{i=1}^{N}(A \cdot \hat{q}_{i+1} \cdot \hat{q}_{i-1} - B \cdot \hat{q}_{i-2} \cdot \hat{q}_{i-1})$
  for $i = 1$ to N **do**
    $\hat{p}_i = -i\hbar \cdot \frac{\partial}{\partial q_i}$
  end for
  $\hat{q}_{N+j} := \hat{q}_j$ for all j
  return $\hat{H}$
end procedure
procedure InitializeQuantumState(N, σ)
  $|\psi_0\rangle = (\pi\sigma^2)^{(-N/4)} \cdot \exp\left(-(q_1^2 + q_2^2 + \cdots + q_N^2)/(2\sigma^2)\right)$
  $|\psi_0\rangle = |\psi_0\rangle / \sqrt{\langle\psi_0|\psi_0\rangle}$
  return $|\psi_0\rangle$
end procedure
procedure GenerateQuantumRandomNumbers
  randomNumbers = empty array of size numRandomNumbers
  $\hat{H}$ = ConvertToQuantumSystem(A, B, N)
  $|\psi\rangle$ = InitializeQuantumState(N, σ)
  for $i = 1$ to numRandomNumbers **do**
    $|\psi\rangle$ = TimeEvolution($|\psi\rangle, \hat{H}$, evolutionTime)
    observableType = (i%2 == 0) ? "*position*" : "*momentum*"
    observableIndex = (i%N) + 1 ▷ Cycle through coordinates
    if observableType == "*position*" **then**
      result, $|\psi\rangle$ = MeasureObservable($|\psi\rangle, \hat{q}_{\text{observableIndex}}$)
    else
      result, $|\psi\rangle$ = MeasureObservable($|\psi\rangle, \hat{p}_{\text{observableIndex}}$)
    end if
    randomValue = ExtractRandomNumber(result, observableType)
    randomNumbers[i] = randomValue
  end for
  return randomNumbers
end procedure
procedure TimeEvolution($|\psi\rangle, \hat{H}, t$)
  $|\psi(t)\rangle = \exp(-i\hat{H}t/\hbar)|\psi\rangle$
  return $|\psi(t)\rangle$
end procedure
procedure MeasureObservable($|\psi\rangle, \hat{O}$)
  for each eigenvalue λ of $\hat{O}$ **do**
    $P(\lambda) = |\langle\lambda|\psi\rangle|^2$
  end for
  result = RandomSampleFrom(eigenvalues, P)
  $|\psi'\rangle = \hat{P}_{\text{result}}|\psi\rangle / \sqrt{\langle\psi|\hat{P}_{\text{result}}|\psi\rangle}$
  return result, $|\psi'\rangle$
end procedure
procedure ExtractRandomNumber(measuredValue, observableType)
  if observableType == "*position*" **then**
    randomDigit = $\left\lfloor \frac{(\text{measuredValue}+3)}{0.6} \right\rfloor$ %10
  else
    randomDigit = $\left\lfloor \frac{(|\text{measuredValue}|+3)}{0.6} \right\rfloor$ %10
  end if
  return randomDigit
end procedure

$Bq_{i-2}q_{i-1}$ interaction. These operations typically involve controlled rotations or multi-qubit gate via controlling gates as sequences to entangle the qubits in a way that reflects the underlying classical coupling dynamics. Once the kinetic and potential parts of the Hamiltonian are represented, the circuit applies the unitary time evolution operator $U = e^{-iHt/\hbar}$. This unitary governs the time dynamics of the entire quantum system and represents the central component of simulating the Hamiltonian evolution on a quantum computer. Eventually, we applied the measurement (M) gates on all qubits in the computational basis to extract the state of the system, allowing analysis of the behavior of the QHC. These outcomes provide probabilistic insights into the evolution of the nD-QHCS.

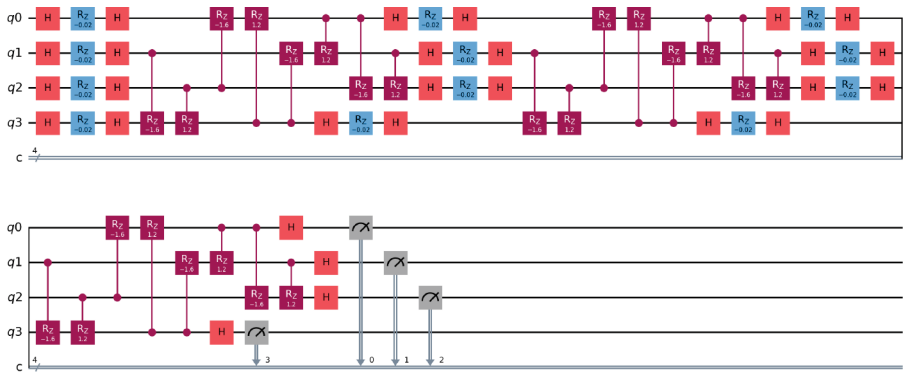


Fig. 2. Quantum circuit of nD-QHCRNG where n=100.

4 Statistical and Analysis

In this section, some testes and the analysis of the work, like bias measurement in random bit sequences, NIST, and entropy are introduced. In addition, we compare our work with other methods.

4.1 Bias Measurement in Bit Strings

Bias is a concept statistical measure of randomness quality in bit sequences. It quantifies the deviation from the ideal 50 − 50 distribution of 0 s and 1 s expected in a truly random binary string. Defined as a mathematical equation:

$$\text{Bias} = \left| \frac{2k}{n} - 1 \right| \tag{14}$$

where n is $\underline{s}$ the total length of the bit string, k is the number of 1 s in the string, and the result ranges from 0 (perfectly balanced) to 1 (completely biased). Table 1 shows the comparison of bias results of the proposed method and other. Figure 3 shows bit-wise bias vs bit position for different QRNG methods.

Table 1. Comparison of Bit-wise Bias and Bias Reduction Techniques

Method	Bit-wise Bias ($\lvert p - 0.5\rvert$)	Bias Reduction Technique	Implementation Technology
nD-QHCRNG	< 0.002 (lowest)	Von Neumann projection	Theoretical model
Standard QRNG [19]	0.002-0.003	Hardware calibration	Optical components
Calude & Svozil [2]	< 0.001	Unitary transformation	3D beam splitters
QRNG with Decoherence [26]	0.002-0.02	Signal whitening	Optical implementations
JUR01 [20]	> 0.05	None (raw output)	Zener diode tunneling
JUR02 [20]	< 0.001	None	Photodiode shot noise
PRNG	0.003-0.013	Mathematical balancing	Software algorithms
SI-QRNG [3]	< 0.0021	Randomness extraction	Silicon polarization decoder
HRNG	0.001-0.013	Hardware whitening	Classical electronic noise

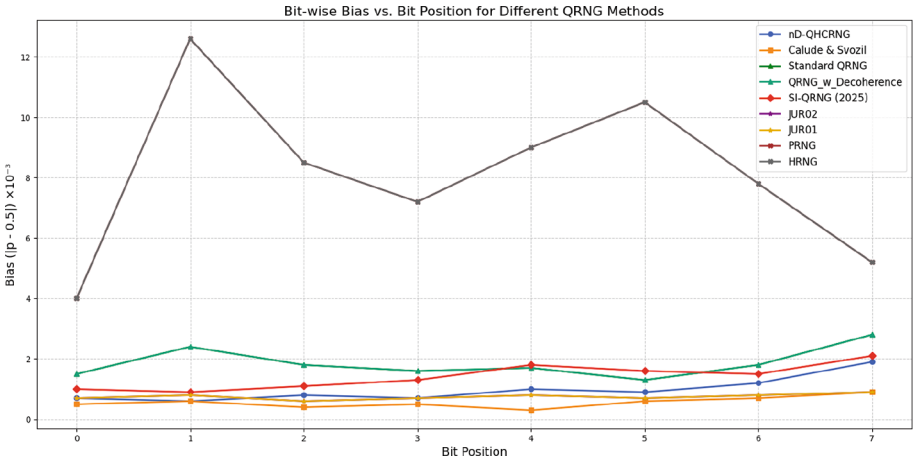


Fig. 3. Bit-wise bias vs bit position for different QRNG methods.

4.2 NIST Tests

A standardized software program for evaluating the random behaviour of time series is provided by the National Institute of Standards and Technology (NIST)

in the United States. The stochastic performance of time series data is evaluated using this software. Several sequences, each with one million bits, are evaluated during the testing procedure. To assess the randomness of the time series, NIST uses two important performance metrics: the pass rate and the P value. The NIST tests the significance threshold (α) is set to 0.01. The confidence interval formula $1 - \alpha \pm 3\sqrt{\alpha(1-\alpha)/m}$ is used to calculate the pass rate. The number of groups of bit sequences is denoted by the symbol m in this formula. When α is 0.01 and m is 100, for example, the resultant confidence interval reduces to the range [0.9602,1.0198], and is $10.01 \pm 3\sqrt{0.01 \times 0.99/100} = 0.99 \pm 0.0094393$. This suggests that the sequence's pass rate needs to be higher than 0.9602 in order to satisfy the necessary requirements. The outcomes of our experiments of NIST tests are shown in Table 2 shows the NIST statistical test for different QRNG methods such as Standard QRNG [19], Calude & Svozil [2], QRNG with Decoherence [26], JUR01 and JUR02 [20], and SI-QRNG [3], PRNG and HRNG.

Table 2. Statistical Test Results (P-values) Comparison

Test	nD-QHCRNG (P-value)	Calude & Svozil [2]	JUR01 & JUR02 [20]	SI-QRNG [3]
Frequency	0.874170	0.261229	0.739918	0.421932
Block Frequency	0.775337	0.692124	0.366918	0.350485
Cumulative Sums	0.186566	0.534146	0.638450	0.662522
Runs	0.486588	0.743917	0.561718	0.415175
Longest Run of Ones	0.647530	0.339308	0.480449	0.697691
Rank	0.246750	0.484646	0.678686	0.544254
FFT	0.152902	0.156856	0.553516	0.366793
Non-overlapping Template	0.691081	0.515989	0.463049	0.485984
Overlapping Template	0.037076	0.214439	0.174249	0.042808
Universal	0.007530	0.122325	0.553516	0.464411
Approximate Entropy	0.440975	0.474986	0.349199	0.464935
Random Excursions	0.141976	0.399413	0.437274	0.446782
Random Excursions Variant	0.066510	0.261101	0.324146	0.553227
Serial	0.119508	0.478136	0.451235	0.258327
Linear Complexity	0.635037	0.200756	0.435840	0.637119
Average P-value	0.316360	0.392092	0.487344	0.462630
Proportion Passed	1.0	1.0	1.0	1.0

4.3 Entropy Analysis

In quantum information theory and quantum systems, VNman entropy [27] is a quantum generalization of classical Shannon entropy. It is named for the mathe-

matician John VNman and quantifies the "mixedness" or uncertainty of a quantum state. The VNman entropy is defined as;

$$S(\rho) = -\operatorname{Tr}(\rho \log \rho)$$

Where Tr represents the trace operation and ρ is the density matrix of our nD − QHCS system. We can demonstrate that:

$$\lim_{n \to 1000} S\left(\rho_{nD-QHCS}\right) \approx \log(d) \tag{15}$$

where d is the dimension of the Hilbert space. This proves near-maximal entropy. Table 3 shows different entropy measurements for several QRNG methods such as; Normalized Shannon Entropy [1], Min-entropy [28], VNman Entropy [27], Rényi Entropy $\alpha = 2$ [29], and Conditional Min-entropy [28].

Table 3. Entropy metrics across different QRNG methods

Method	Normalized Shannon Entropy (%)	Min-entropy	VNman Entropy	Rényi Entropy ($\alpha = 2$)	Conditional Min-entropy	Extraction Efficiency (%)
nD-QHCRNG	99.7	0.992	0.996	0.991	0.990	99.2
Standard QRNG [19]	98.2	0.965	0.978	0.963	0.960	96.5
Calude & Svozil [2]	99.1	0.992	0.993	0.990	0.989	99.0
QRNG with Decoherence [26]	94.5	0.908	0.932	0.901	0.897	90.5
JUR01 [20] (raw)	85.3	0.795	0.822	0.783	0.776	78.2
JUR02 [20]	99.2	0.989	0.991	0.987	0.985	98.7
PRNG	92.5	0.885	0.912	0.879	0.872	88.1
SI-QRNG [3]	99.3	0.994	0.995	0.992	0.991	99.1
HRNG	93.1	0.897	0.925	0.891	0.885	89.3
Theoretical Maximum	100.0	1.000	1.000	1.000	1.000	100.0

4.4 Autocorrelation Functions

Autocorrelation tests are one important statistical test used to check the randomness quality of QRNGs. They measure how similar a sequence is to itself when shifted by a certain number of positions. The autocorrelation at lag k is calculated as;

$$R(k) = \Sigma\left(x_{\mathrm{i}} - \mu\right)\left(x_{\mathrm{i+k}} - \mu\right) / \Sigma\left(x_{\mathrm{i}} - \mu\right)^2 \tag{16}$$

where x_i are the binary sequences where $i = 1 \ldots n$ (n is the length of the binary sequence), μ is the mean of the sequence, and k is the lag (number of positions to shift) [31]. Figure 4 explained, where $R(0) = 1$ is mean always true randomness, as a sequence perfectly correlates with itself at lag 0, while $R(k) \approx 0$ for $k > 0$ mean is random sequences, values should be near zero for all nonzero lags, where the positive values indicate similar patterns repeating at that lag, and negative values are indicate inverse patterns at that lag, and the confidence band 95% is typically set at $\pm 1.96/\sqrt{n}$.

5 Discussion

The results based on the proposed analysis highlight the effectiveness of the nD − QHCRNG method in generating high quality random numbers, which can be used in various fields such as cryptography, physics, and others, as mentioned in the introduction regarding the benefits of PRNGs in different domains. The bias measurements, consistently demonstrate that nD − QHCS achieves a lower bias compared to other QRNG techniques beside the classical PRNGs methods. Therefore, this indicates a more uniform distribution of 0 s and 1 s, which is crucial issue for other fields such as cryptography, physics, and different applications. For further support, Table 1 shows that the nD-QHCS consistently has the lowest bit-wise bias (< 0.002). The VNman projection measurement technique is key to this low bias. The NIST tests further validate the randomness of the generated bit sequences. As shown in Table 2, the nD-QHCS method successfully passes all the NIST SP 800-22 tests, confirming its suitability for applications requiring stringent randomness criteria. When the average P-value of 0.316360 and proportion passed of 1.0, this means that our proposal has strong performance across the NIST suite. Entropy analysis illustrates that the nD-QHCRNG method exhibits near-maximal entropy, approaching the theoretical maximum as shown in Table 3. The normalized Shannon entropy is 99.7%, and the VNman entropy is 0.996, both very close to the ideal 100% and 1.000, respectively. This high entropy signifies a high degree of unpredictability and randomness in the generated numbers. Finally, the autocorrelation analysis demonstrates that the nD-QHCS method has negligible autocorrelation, especially at higher lags (Fig. 4). This confirms that the generated random numbers are statistically independent, a critical property for many applications. The autocorrelation values are near zero for lags greater than 5.

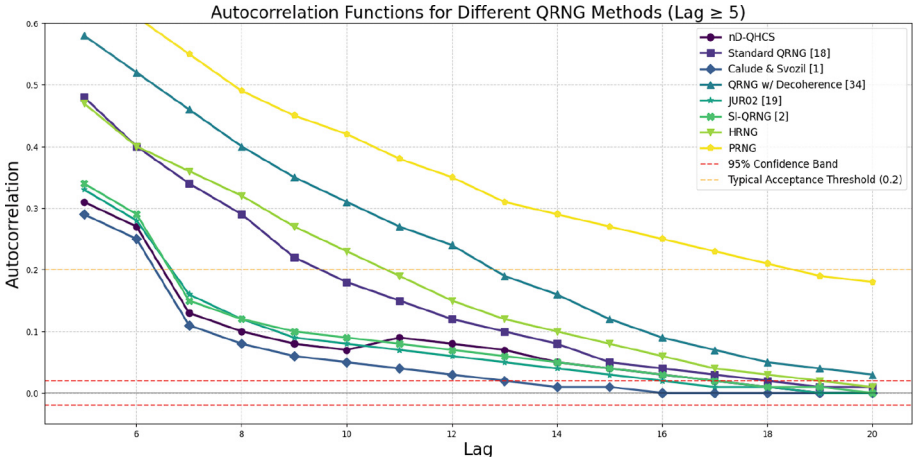


Fig. 4. Autocorrelation test for different QRNG methods (Lag ≥ 5).

6 Conclusion

In this work, a new quantum random number generation method based nD quantum hyperchaotic system, nD-QHCRNG, is presented. The VNman projection measurement was used to measure the properties corresponding to different values of the Hamiltonian in the nD-QHCS. The results of the statistical analysis based on our method demonstrate that the nD-QHCRNG generates high-quality random numbers with low bias, passes all NIST tests, exhibits near-maximal entropy, and shows negligible autocorrelation, indicating that our model is well-suited for use in various fields requiring pseudorandom number generation (PRNG), whether classical or quantum in the future. Based on these statistical tests, we have several properties that make it a promising candidate for applications requiring strong randomness, such as cryptography, scientific simulations, and artificial intelligence. Specifically, the bit-wise bias is consistently below 0.002 and the normalized Shannon entropy reaches 99.7%. The nD-QHCRNG method combines the sensitivity to initial conditions characteristic of classical nD-HCS [1] with the fundamental indeterminism of quantum measurement, leveraging the chaotic behavior of qubits in quantum mechanics, resulting in a QRNG with performance that meets or exceeds other state-of-the-art methods. Future work could focus on further optimizing the system and exploring its implementation in practical quantum computing platforms.

References

1. Alwan, N.A., Obaiys, S.J., Noor, N.F.B.M., Al-Saidi, N.M., Karaca, Y.: Color image encryption through multi-S-box generated by hyperchaotic system and mixture of pixel bits. Fractals 2440039 (2024)

2. Calude, C.S., Svozil, K.: Binary quantum random number generator based on value indefinite observables. Sci. Rep. **14**(1), 12845 (2024)
3. Du, Y., et al.: Source-independent quantum random number generators with integrated silicon photonics. Commun. Phys. **8**(1), 9 (2025)
4. Hensen, B., et al.: Loophole-free Bell inequality violation using electron spins separated by 1.3 km. Nature **526**(7575), 682–686 (2015)
5. Giustina, M., et al.: Significant-loophole-free test of Bell's theorem with entangled photons. Phys. Rev. Lett. **115**(25), 250401 (2015)
6. Liu, L., et al.: A post-processing method for quantum random number generator based on zero-phase component analysis whitening. Entropy **27**(1), 68 (2025)
7. Lebedev, A., Möslein, A., Yaman, O.I., Rajan, D., Intallura, P.: Effects of the entropy source on Monte Carlo simulations. arXiv preprint arXiv:2409.11539 (2024)
8. Herrero-Collantes, M., Garcia-Escartin, J.C.: Quantum random number generators. Rev. Mod. Phys. **89**(1), 015004 (2017)
9. Ma, X., Yuan, X., Cao, Z., Qi, B., Zhang, Z.: Quantum random number generation. NPJ Quantum Inform. **2**(1), 1–9 (2016)
10. DiCarlo, D.F.: Random number generation: Types and techniques (2012)
11. Calude, C.S.: Information and randomness: an algorithmic perspective. Springer Science & Business Media (2013)
12. Pironio, S., et al.: Random numbers certified by Bell's theorem. Nature **464**(7291), 1021–1024 (2010)
13. Nonaka, M., Agüero, M., Kovalsky, M., Hnilo, A.: Testing randomness of series generated in an optical Bell's experiment. Appl. Opt. **62**(12), 3105–3111 (2023). https://doi.org/10.1364/AO.477218
14. Abbott, A.A., Calude, C.S., Conder, J., Svozil, K.: Strong Kochen-Specker theorem and incomputability of quantum randomness. Phys. Rev. A **86**(6), 062109 (2012)
15. Abbott, A.A., Calude, C.S., Svozil, K.: A variant of the Kochen-Specker theorem localising value indefiniteness. J. Math. Phys. **56**(10) (2015)
16. Alwan, N.A., Obaiys, S.J., Al-Saidi, N.M., Noor, N., Karaca, Y.: A pseudo random number generator based on 4D hyperchaotic systems, riddled basins of attraction and advanced microfluidic technology. In: International Conference on Computational Science and Its Applications, pp. 91–109. Springer (2024)
17. Haider, T., Blanco, S.A., Hayat, U.: A Novel Pseudo-Random Number Generator Based on Multi-Objective Optimization for Image-Cryptographic Applications. arXiv preprint arXiv:2307.03911 (2023)
18. Al-dabbas, H.M., Ajaj, A.M., Al-Saidi, N.M., Alwan, N.A., El Sobky, W.I.: A quantum-corrected chaotic system for strengthening Schnorr and Elgamal signatures to optimize key generation and performance. Int. J. Anal. Appl. **23**, 65–65 (2025)
19. Heese, R., Wolter, M., Mücke, S., Franken, L., Piatkowski, N.: On the effects of biased quantum random numbers on the initialization of artificial neural networks. Mach. Learn. **113**(3), 1189–1217 (2024)
20. Jacak, M.M., Jóźwiak, P., Niemczuk, J., Jacak, J.E.: Quantum generators of random numbers. Sci. Rep. **11**(1), 16108 (2021)
21. https://www.python.org/downloads/release/python-3110/
22. Chen, G., et al.: Quantum computing devices: principles, designs, and analysis. Chapman and Hall/CRC (2006)
23. Landau, L., Lifshitz, E.: Quantum Mechanics (Non-relativistic Theory). Pergamon, New York (1977)

24. Mermin, N.D.: Physics: QBism puts the scientist back into science. Nature **507**(7493), 421–423 (2014)
25. Kolmogorov, A.N.: On tables of random numbers. Theoret. Comput. Sci. **207**(2), 387–395 (1998)
26. Grigoryan, A.M., Agaian, S.S.: Quantum Image Processing in Practice: A Mathematical Toolbox. John Wiley & Sons (2025)
27. Svozil, K.: Three criteria for quantum random-number generators based on beam splitters. Phys. Rev. A **79**(5), 054306 (2009)
28. Masood, S.S., Miller, A.: A Von Neumann Entropy Measure of Entanglement Transfer in a Double Jaynes-Cummings Model. arXiv preprint arXiv:1412.5410 (2014)
29. Yang, J., et al.: Neural network based min-entropy estimation for random number generators. In: International Conference on Security and Privacy in Communication Systems, pp. 231–250. Springer (2018)
30. Fehr, S., Berens, S.: On the conditional Rényi entropy. IEEE Trans. Inf. Theory **60**(11), 6801–6810 (2014)
31. Wilde, F., Frisch, C., Pehl, M.: Efficient bound for conditional min-entropy of physical unclonable functions beyond IID. In: 2019 IEEE International Workshop on Information Forensics and Security (WIFS), pp. 1–6. IEEE (2019)
32. Faure, E., Myronets, I., Lavdanskyi, A.: Autocorrelation criterion for quality assessment of random number sequences. In: CMIS, pp. 675–689 (2020)