Cumhuriyet Sci. J., 46(3) (2025) 891-901
DOI: https://doi.org/10.17776/csj.1557049

Cumhuriyet Science Journal

| csj.cumhuriyet.edu.tr | Founded: 2002 ISSN: 2587-2680 e-ISSN: 2587-246X Publisher: Sivas Cumhuriyet University

Design and Analysis of a Quadratic Lorenz-like Attractor for Pseudo-Random Number Generation

Buğçe Eminağa Tatlıcıoğlu[1, a,*], Hatice Aktöre[1,b]

[1]*Department of Basic Sciences and Humanities, Faculty of Art and Sciences, Cyprus International University, Nicosia, Northern Cyprus, via Mersin 10, Turkey*

**Corresponding author*

Research Article

History
Received: 27/09/2024
Accepted: 27/11/2025

ABSTRACT

This study introduces and analyzes a novel quadratic Lorenz-like attractor and demonstrates its application as a pseudo-random number generator (PRNG). A theoretical and numerical investigation of the system dynamics is conducted, including equilibrium point analysis, Jacobian eigenvalues, dissipativity, and Lyapunov exponents. The results indicate that the quadratic modification alters the system dynamics, producing stronger chaotic intensity than the classical Lorenz system. This is supported by larger positive Lyapunov exponents and a non-integer Lyapunov dimension (≈2.40), which reflects a more complex attractor geometry. Numerical simulations, time series, phase projections, and bifurcation analysis further illustrate the rich nonlinear dynamics of the system. To validate its applicability, the chaotic sequences generated by the attractor were subjected to standard statistical evaluations, including the NIST SP800-22, Diehard, and ENT test suites. A dataset of 18 million samples was employed, significantly exceeding the minimum requirement for meaningful validation, and the results confirm that the proposed generator produces high-quality randomness. The importance of this work lies in demonstrating that the quadratic Lorenz-like attractor offers both strong chaotic intensity and relatively simple structure, making it a promising candidate for cryptographic applications, secure communications, and other domains requiring reliable pseudo-random number generation.

Keywords: Chaos Theory, Random number generation, Dynamical system, Lorenz attractor

[a] *btatlicioglu@ciu.edu.tr* *https://orcid.org/0000-0001-8854-4464* [b] *haktore@ciu.edu.tr* *https://orcid.org/0000-0003-2455-3681*

Introduction

The creation of random numbers has become a necessary tool well beyond its statistical significance in simulations with the introduction of public-key cryptography by W. Diffie and M. Hellmann [1] and its most notable representation, the RSA-Algorithm [2, 3]. Since it is not particularly practical or readily available to generate "real" random numbers by the measurement of physical system features, such as ionization radiation using a Geiger-Mueller counter or white noise in a variety of physical systems.

Therefore, the practical implementation of public-key cryptography-based encryption systems requires readily available and disposable pseudo-random number generators. Using chaotic systems is one way to obtain statistically uncorrelated pseudo-random numbers [4, 5, 6, 7, 8, 9].

Recent advances continue to highlight the role of chaotic systems in pseudo-random number generation. For example, Lynnyk, Sakamoto, and Čelikovský [10] proposed GLS-based algorithms that exploit all three coordinates of the generalized Lorenz system, demonstrating strong statistical properties and resistance to brute-force attacks. Similarly, Cho and Miyano [11] developed a chaos-based stream cipher using an augmented Lorenz star network, with randomness validated by both NIST SP800-22 and TestU01 test suites. In another line of research, Ebrahimzadeh and Jampour [12] introduced a chaotic genetic algorithm that employs Lorenz-based pseudo-random sequences to overcome local convergence in optimization problems, achieving better efficiency than traditional genetic algorithms. Complementing these application-driven studies, Abdelhaleem, Abd-El-Hafiz, and Radwan [13] recently provided a comprehensive analysis of both chaotic and non-chaotic PRNG design scenarios, offering guidelines and confirming through extensive statistical testing that well-designed PRNGs can meet international cryptographic standards. Together, these works reinforce the importance of exploring new chaotic attractors for secure and efficient pseudo-random number generation, which serves as the motivation for the present study.

Unlike previous studies that employed generalized Lorenz systems [10] or star networks of Lorenz oscillators [11], the present work introduces a quadratic Lorenz-like attractor with distinct nonlinear dynamics. The quadratic modification strengthens the chaotic intensity, as confirmed by Lyapunov exponents and fractional dimension, and enables the generation of pseudo-random sequences that successfully pass NIST, Diehard, and ENT tests. This demonstrates that a mathematically simple yet novel attractor can serve as a promising alternative for secure pseudo-random number generation.

Mathematical models known as dynamic systems use equations of motion with sensitive beginning values to describe the temporal evolution of a system. Applications of dynamical systems may be found, for example, in

population dynamics in biology [14], chemical kinetics in chemistry [15, 16], and many fields of physics [17, 18, 19]. Mathematical economy and finance are two examples of topics outside of mathematics and the natural sciences where dynamic systems theory has been used [20, 21, 22].

With his pioneering work in 1890, Poincaré gave the field of dynamical systems a big start [23]. Afterwards, in the 1920s, the dynamics of complex analytic maps were presented by [24] and [25]. Studies like [26], [27, 28, 29], Cartwright and Littlewood [30] have their roots in physics, such as the astronomical three body issue. On the other hand, Stephan Smale provided a method that was solely driven by mathematics [31, 32]. Very basic differential equations can turn chaotic in some situations, according to E. N. Lorenz [18]. The system put out by Lorenz exhibits the wellknown two scroll butterfly structure in addition to an extremely sophisticated dynamical behavior. The Lorenz system's dynamic equations are provided as

$$\frac{dx}{dt} = \sigma(y - x) \tag{1}$$

$$\frac{dy}{dt} = x(\rho - z) - y \tag{2}$$

$$\frac{dz}{dt} = xy - \beta z \tag{3}$$

where it is assumed that σ, ρ, and β are all positive parameters. Lorenz exemplified the chaotic behavior of the system with the constants σ = 10, β = 8/3, and ρ = 28. Another seminal work in the study of 3D dynamic systems is Rössler's investigation of "The equation for continuous chaos" [17]. Two unstable saddle-foci are a trait shared by the Burke Shaw system [33] and the Rossler attractor. Chen [34] and Lü and Chen [35] have postulated other chaotic systems that, while not topologically identical, have a basic structure similar to that of the Lorenz system. The transition between Lorenz and Chen attractors is discussed by Lü and Chen [35]. Another chaotic system with three fixed points one saddle and two stable fixed points was also presented by Yang and Chen. Similar to the Lorenz, Chen, and Yang-Chen systems, Yang et al. [36] and Pehlivan et al. [37] presented and analyzed chaotic systems having two distinct fixed points, or two stable node-foci. Numerous technical applications, including electrical circuits, have also included chaotic systems [38, 39]. Different Non-Newtonian Calculi, such as fractional calculus, geometric multiplicative calculus, and bigeometric multiplicative calculus, have also been used to explain dynamic systems. In order to statistically investigate the chaotic behavior of the fractional order of the Lü system, Jun Guo Lü converted the Lü system into fractional calculus [40].

In order to improve security, random number generators, or RNGs, are employed in information technology, especially in security related applications like cryptography. Several statistical tests are used to evaluate the generated data's unpredictability. A lengthy series of produced numbers must make up the tested experimental data.

The statistical test suite SP 800-22 [41], which was most recently amended in April 2010 and initially released by the U.S. National Institute of Standards and Technology (NIST) in 2001, is the subject of this work. An n-bit sequence is the input for each of the 15 p-value based tests in the test suite. This work presents a novel chaotic attractor that is discovered by adding a quadratic component to the Lorenz system. Thorough numerical and theoretical examination indicates that the suggested system exhibits chaotic characteristics and possesses the characteristics of a two-scroll attractor, akin to the Lorenz attractor. It is well recognized that more chaos in the systems leads to more secure outcomes. In this way, the recently suggested approach is used to generate a random number generator, and the NIST statistical test suite is used to confirm that the generated RNGs are applicable.

In Section 2, the modified quadratic Lorenz attractor is presented and its features are discussed and analyzed through theoretical and numerical determination of the equilibria points and Lyapunov exponents. The randomness of the RNGs and the generator created using the modified quadratic Lorenz attractor are examined in Section 3. The conclusion of this study provides an overview of the findings.

Design of a new Chaotic System

We will suggest and explain a novel chaotic system that follows the Lorenz attractor in the following. This is the suggested system:

$$\frac{dx}{dt} = \sigma(yz - x) \tag{4}$$

$$\frac{dx}{dt} = \rho x - xz \tag{5}$$

$$\frac{dz}{dt} = (xy)^2 - \beta z \tag{6}$$

where σ, ρ, and β are real parameters, and x, y, and z are state variables. Each equation in the newly proposed chaotic system differs in certain aspects from the original Lorenz system. A term by term comparison of equations (1)–(3) with equations (4)–(6) highlights these variations. In the original Lorenz system, equation (4) is nonlinear, whereas its counterpart, equation (1), in the proposed system is linear. Similarly, equations (2) and (5) are both nonlinear; however, the y-dependence present in equation (2) is absent in equation (5). The most significant distinction is observed when comparing equations (3) and (6): in equation (6), the term xy is squared, unlike the corresponding linear term in equation (3).

Table 1: Comparison of Original Lorenz System and Proposed Quadratic Lorenz-like System

Equation	Lorenz System	Quadratic Lorenz-like System	Key Difference
(1) vs (4)	$\dot{x} = \sigma (y - x)$	$\dot{x} = \sigma (yz - x)$	Linear in x for proposed system; original has y-x coupling
(2) vs (5)	$\dot{y} = x(\rho - z)-y$	$\dot{y} = (\rho - z)x$	Both nonlinear, but explicit y-dependence is removed
(3) vs (6)	$\dot{z} = xy - \beta z$	$\dot{z} = (xy)^2 - \beta z$	Quadratic modification: xy term is squared, increasing nonlinearity

To highlight the structural differences between the classical Lorenz system and the proposed quadratic Lorenz-like system, a side by side comparison of their governing equations is provided in Table 1. While both systems share the same parameters (σ,ρ,β) and state variables (x,y,z) each equation in the quadratic variant introduces specific modifications. These differences, particularly the replacement of the xy-term with the $(xy)^2$, result in enhanced nonlinearity and contribute to stronger chaotic behavior.

System Description

The proposed quadratic Lorenz-like system is obtained by modifying the structure of the classical Lorenz system through the introduction of nonlinear coupling and a quadratic term. The governing equations of the system are expressed as:

$$\begin{aligned} \frac{dx}{dt} &= \sigma(yz - x) \\ \frac{dy}{dt} &= \rho x - xz \\ \frac{dz}{dt} &= (xy)^2 - \beta z \end{aligned} \tag{7}$$

where σ, ρ, and β are real valued parameters, and x, y, and z are the system state variables. Each equation differs from the original Lorenz system, with the most notable modification being the quadratic term $(xy)^2$ in the third equation, which introduces an additional degree of nonlinearity.

This system exhibits cylindrical symmetry under the transformation $(x, y, z) \rightarrow (-x, -y, z)$ a property that persists for all parameter values. The presence of quadratic nonlinearity enhances the chaotic intensity of the system while retaining a relatively simple mathematical form. This makes it well suited for applications such as pseudo-random number generation, where both unpredictability and computational efficiency are crucial.

For varying values of β and fixed values σ = 12 and $\beta = 4$, the proposed non-linear attractor (4)-(6) is solved for the initial values (1, 1, 1). As shown in figure 1, the chaotic behavior only appears for certain values of ρ.

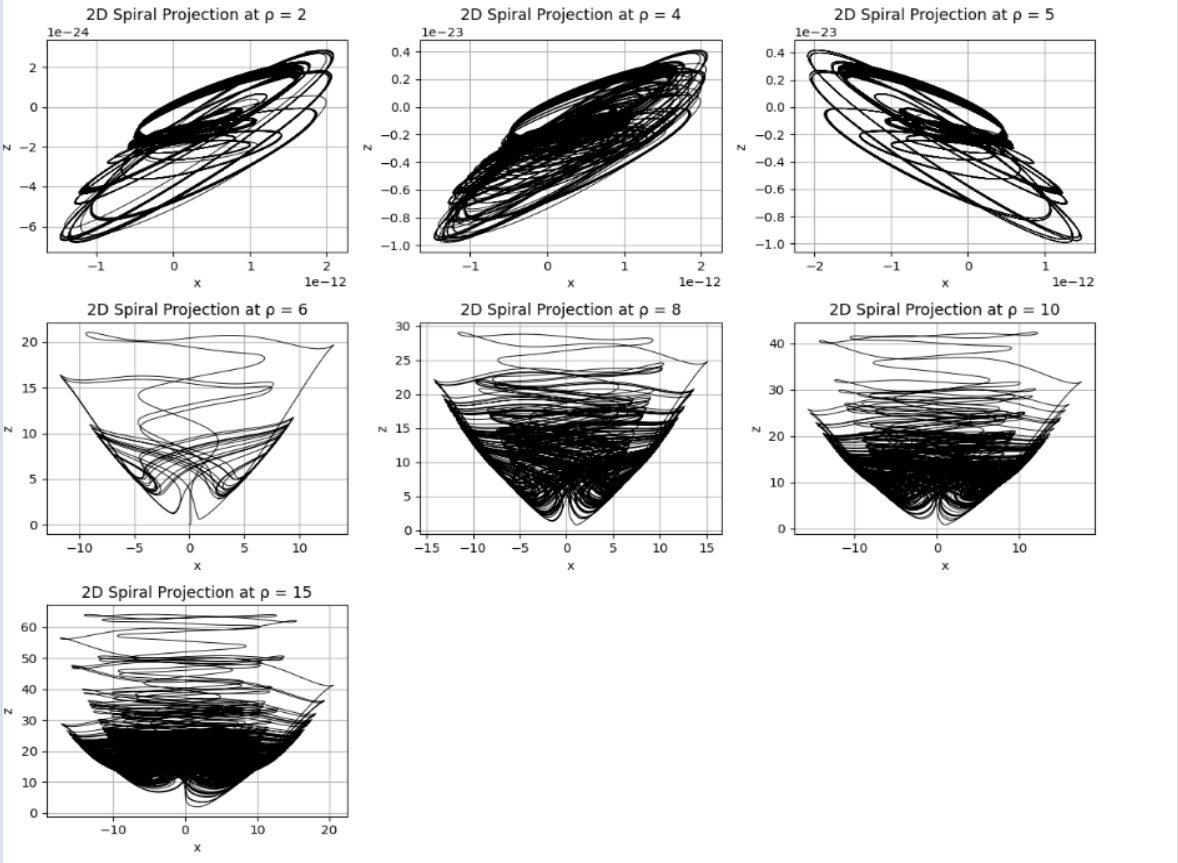

Figure 1: Simulation of the system when σ = 12, $\beta = 4$and various ρ parameter values

As the control parameter ρ is varied, the system exhibits a bifurcation sequence that marks the progression from near equilibrium dynamics to chaotic behavior. For low values of ρ (e.g., 2, 4, 5), the trajectories remain confined in the vicinity of the origin, producing minute oscillations that appear as highly compressed spirals in phase space. This reflects the presence of a stable equilibrium state, where the dynamics are dominated by damped oscillations rather than sustained motion. As ρ increases to intermediate values (6, 8, 10), the system undergoes a qualitative change: the oscillations grow in amplitude, giving rise to spiral funnels and increasingly dense attractor bands. In this regime, the trajectories no longer converge to a fixed point but instead explore an extended region of state space, indicative of the onset of chaotic dynamics. For higher values, such as $\rho = 15$, the attractor undergoes further structural changes, evolving into a fully developed chaotic set characterized by overlapping sheets and layered structures in the x–z projection. The trajectories remain bounded yet non-periodic, and the darker regions correspond to areas of higher invariant measure where the system spends a significant proportion of time. Taken together, these results demonstrate a clear route to chaos through successive bifurcations, highlighting the transition from equilibrium states to oscillatory regimes and finally to chaotic attractors as ρ increases.

System Analysis

Equilibrium points

The first step to analyze a chaotic system is to find the equilibrium points. It is well known that the system is in equilibrium, when $\dot{x}$, $\dot{y}$, $\dot{z}$ vanish. Therefore, the equilibrium points of the proposed system (4)-(6) are given by the solution of the following set of equations with respect to x, y, z as following.

$$\begin{aligned} &\sigma(yz - x) = 0 \\ &\rho x - xz = 0 \\ &(xy)^2 - \beta z = 0 \end{aligned} \tag{8}$$

Thus, the solution of the system (8) with respect to x, y, z gives the equilibrium points as:

$$O = (0,0,0)$$

$$E^+ = \left(\sqrt[4]{\beta\rho^3}, \sqrt[4]{\frac{\beta}{\rho}}, \rho \right)$$

$$E^- = \left(-\sqrt[4]{\beta\rho^3}, -\sqrt[4]{\frac{\beta}{\rho}}, \rho \right)$$

For the chosen parameters $\beta = 4, \sigma = 12$ and $\rho = 8$, the numerical values of the equilibrium points yield to

$$O = (0,0,0) \tag{9}$$

$$E^+ = (6.73, 0.84, 8) \tag{10}$$

$$E^- = (-6.73, -0.84, 8) \tag{11}$$

Stability

For the decision of the stability of the proposed system, the eigenvalues of the Jacobian have to be analyzed. The Jacobian for this system (4)-(6) can be easily obtained as

$$J = \begin{bmatrix} \partial_x\dot{x} & \partial_y\dot{x} & \partial_z\dot{x} \\ \partial_x\dot{y} & \partial_y\dot{y} & \partial_z\dot{y} \\ \partial_x\dot{z} & \partial_y\dot{z} & \partial_z\dot{z} \end{bmatrix} = \begin{bmatrix} -\sigma & \sigma z & \sigma y \\ \rho - z & 0 & -x \\ 2xy^2 & 2x^2y & -\beta \end{bmatrix} \tag{12}$$

The general closed form expressions for the eigenvalues of the Jacobian matrix (12) are very long and complicated. As we are only interested in the numerical values of the eigenvalues at the equilibrium points (9)-(11) for the given parameters $\beta = 4, \sigma = 12$ and $\rho = 8$, the eigenvalues are stated in table 2:

Table 2: Eigenvalues of the Jacobian at the equilibrium points

Equilibrium Point	λ_1	λ_2	λ_3
O	−12	−4	0
E^+	2.65 + 23.87i	2.65 −23.87i	−21.3
E^-	2.65 + 23.87i	2.65 −23.87i	−21.3

At the origin O, the eigenvalues are λ_1=−12, λ_2=−4 and λ_3=0. Since two eigenvalues are negative and one is zero, the origin represents a non-hyperbolic equilibrium point and is therefore unstable.

For the equilibria $E^+$and E^-, the eigenvalues are identical due to the quadratic symmetry of the system. In both cases, λ_1 and λ_2 are complex conjugates with positive real parts, while λ_3 is a negative real number. The presence of eigenvalues with positive real parts confirms that both $E^+$and E^- are unstable equilibrium points [42]

Bifurcation Analysis

Bifurcation analysis is an important tool for understanding the qualitative changes in the dynamics of nonlinear systems as parameters vary. In chaotic systems, small variations in control parameters can lead to dramatic changes in system behavior, such as transitions from stable fixed points to periodic oscillations and eventually to chaotic attractors. To investigate the influence of system parameters on the proposed quadratic Lorenz-like system, we performed a bifurcation study by varying the parameter ρ while keeping σ=12 and β=4 fixed.

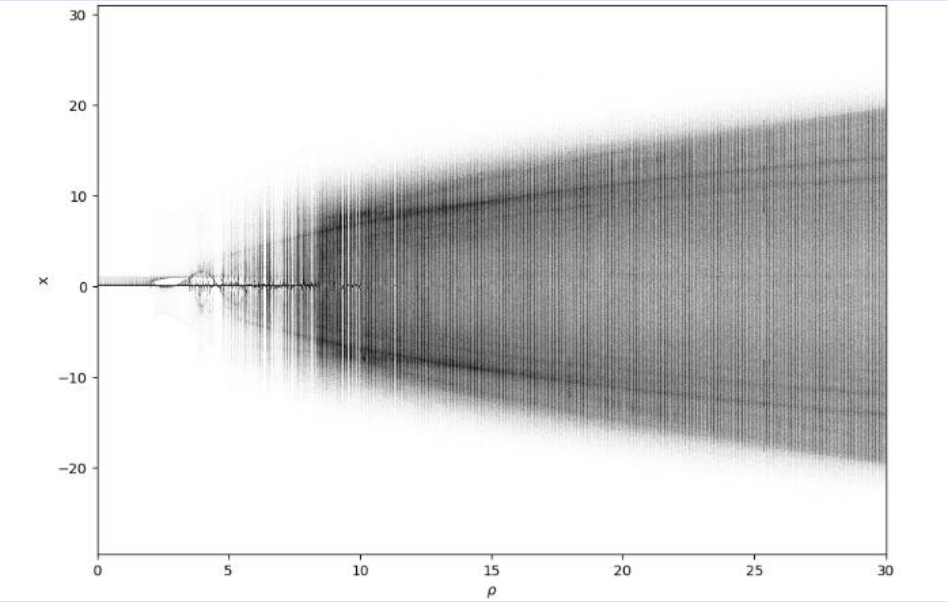

Figure 2: Bifurcation diagram for σ=12, β=4 and varying ρ

Figure 2 presents the bifurcation diagram of the system, where the long term values of the state variable x are plotted as a function of ρ. To eliminate transient effects, the initial portion of each trajectory was discarded, and only the asymptotic states were recorded. This allows the bifurcation structure of the system to be clearly observed.

The bifurcation diagram in Figure 2 illustrates several distinct dynamical regimes:

- Stable region at small ρ: For values of ρ close to zero, the system settles to equilibrium, with x→0. This indicates that the system is stable and non-chaotic in this range.
- Onset of instability $(\rho \approx 4 - 6)$: As ρ increases, small oscillations and fluctuations in x emerge. This corresponds to the loss of stability of the equilibrium state and the onset of periodic oscillations.
- Transition to complex dynamics $(\rho > 6)$: Beyond this threshold, the diagram shows increasingly dense bands of x-values, characteristic of period doubling bifurcations leading to chaos. The state variable oscillates irregularly over a wide range, reflecting the system's entry into chaotic regimes.
- Fully developed chaos $(\rho \gtrsim 10)$: For larger values of ρ, the diagram becomes a filled region where x spans a broad continuous interval. This indicates fully developed chaotic behavior, where the trajectory is highly sensitive to initial conditions and explores a wide range of states.

Overall, the bifurcation diagram confirms that the quadratic Lorenz-like system exhibits the hallmarks of nonlinear chaotic dynamics, including equilibrium stability loss, transition through oscillatory states, and fully developed chaos as ρ increases. Such parameter dependent transitions are critical in evaluating the system's potential for pseudo-random number generation, since chaos is directly linked to unpredictability and complexity in the output sequences.

Symmetry and Dissipativity

The system defined by equations (4)–(6) possesses cylindrical symmetry, meaning it remains invariant under the coordinate transformation (x,y,z)→(−x,−y,z) and this property holds for all values of the system parameters.

To examine the dissipativity of the system (4)–(6), we first define the corresponding vector field F as:

$$F\ (\dot{x}, \dot{y}, \dot{z})^T \tag{13}$$

with $(\dot{x}, \dot{y}, \dot{z})$ from (4)-(6). Then we get for the volume change rate

$$\Lambda = div\, \boldsymbol{F} = -(\sigma + \beta). \tag{14}$$

where $\beta = 4, \sigma = 12$ and $\rho = 8$, the volume change rate becomes $\Lambda = -(12 + 4) = -16$. As $\Lambda < 0$, the system is identified as dissipative [10] and the volume contracts exponentially as:

$$V\ (t) = V_0 e^{\Lambda t} = V_0 e^{-16t} \tag{15}$$

From (14), it can be seen that a volume element V_0 is contracted by the flow into a volume element $V_0 e^{-16t}$ at the time t.

Lyapunov Exponent and Fractional Dimension

Lyapunov exponents generally refer to the average exponential rates of divergence or convergence of nearby trajectories in the phase space. The important part is that if there is at least one positive Lyapunov exponent, the system can be defined to be chaotic. According to the detailed numerical and theoretical analysis, the Lyapunov exponents are found to be l_1 = 5.4162, l_2 = 2.1912, and l_3 = −19.2269. The Lyapunov dimension, introduced by Kaplan and Yorke [44], is considered as measure for the chaotic behaviour of the attractor.

If we are dealing with a chaotic deterministic system, the Lyapunov dimension is generally non-integer. In order to calculate the Lyapunov dimension in the Kaplan-Yorke framework, first we have to make sure that the Lyapunov exponents are indexed in decreasing order, i.e.

$l_1 \geq l_2 \geq l_3$,

which has already been done in our case. First we have to determine the index j such that

$$\sum_{i=1}^{j} l_i > 0, \quad and \quad \sum_{i=1}^{j+1} l_i < 0$$

Obviously, the index j = 2. Then the conjecture is that the dimension of the attractor is

$$D_L = j + \frac{\sum_{i=1}^{j} l_i}{|l_{j+1}|} = 2.3957 \tag{16}$$

Since the Lyapunov dimension is in the range $2 < D_L < 3$, the result is consistent with the findings in [45]. Equation (15) means that the system (4)-(6) is a dissipative system, and the Lyapunov dimensions of the system are fractional. Having a strange attractor and positive Lyapunov exponent, it is obvious that the system is a 3D chaotic system.

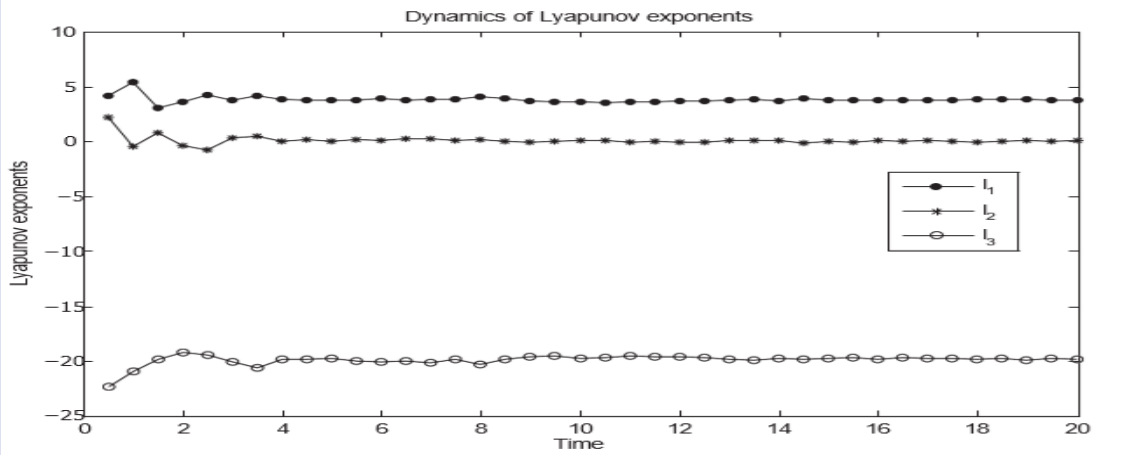

Figure 3: Plot of Lyapunov exponents

Figure 3 shows that the three Lyapunov exponents $(\lambda_1, \lambda_2, \lambda_3)$ of the proposed system stabilize after an initial transient. One exponent remains positive, one is approximately zero, and the third is negative. This configuration demonstrates sensitivity to initial conditions, dissipativity, and the existence of a strange attractor, confirming that the system exhibits 3D chaotic behavior with a fractional Lyapunov dimension.

Numerical Simulations

Time series analysis of the system (4)-(6) yielded the individual plots of x(t), y(t), z(t) as shown in Figure 4. For the solutions of the system the Runge-Kutta method was employed.

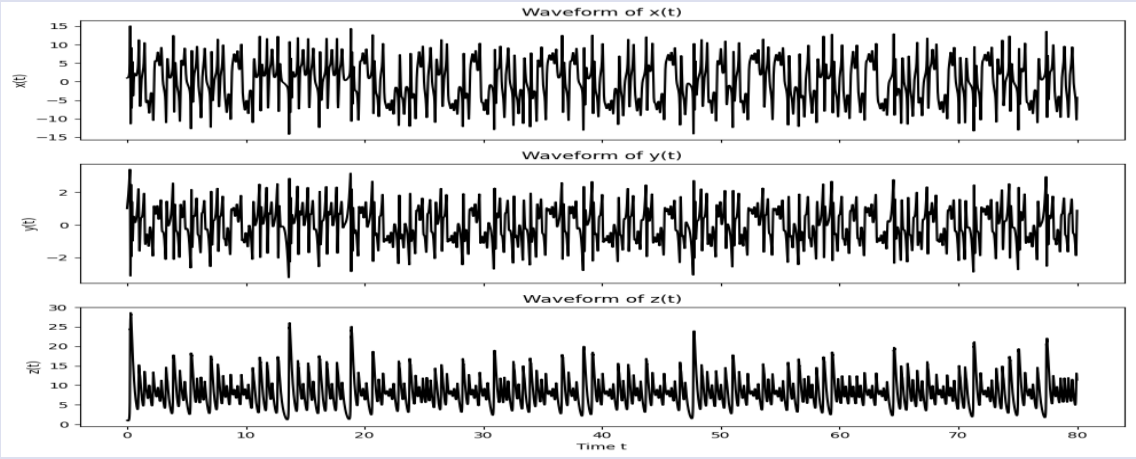

Figure 4: Waveforms of *x*(*t*), *y*(*t*), *z*(*t*) respectively

The time domain waveforms of the system states x(t),y(t),z(t) are shown in Fig. 4. Each state exhibits irregular, non-repetitive oscillations that are characteristic of chaotic dynamics. The waveform of x(t) demonstrates large fluctuations around zero with no observable periodicity, while y(t) shows similarly irregular

oscillations with varying amplitude. The waveform of z(t) differs slightly in that it remains strictly positive and oscillates with strong irregular bursts. Together, these time series confirm the non-periodic and unpredictable nature of the quadratic Lorenz-like system, which is essential for pseudo-random number generation.

The projections of the system (4)-(6), on the various axes are given in Figure 5.

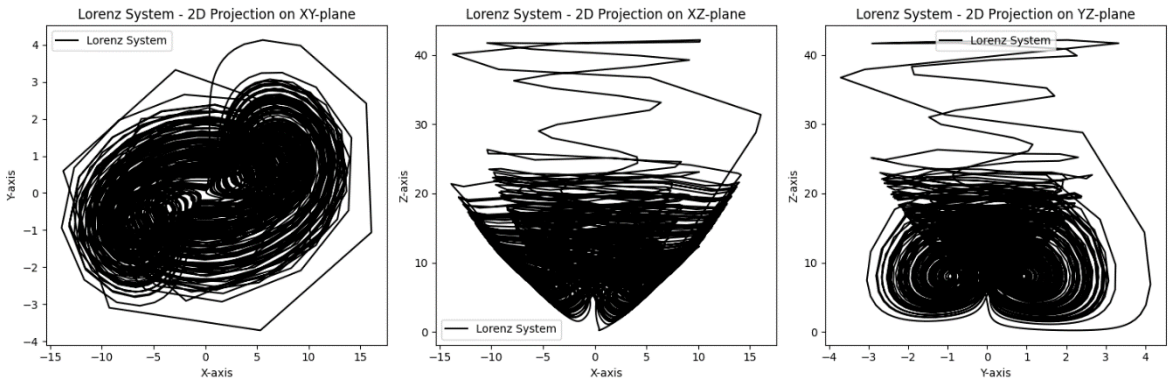

Figure 5: Projection of System (4-6) on the xy-plane, xz-plane and yz-plane respectively

The two-dimensional projections of the trajectories onto the x–y, x–z, and y–z planes are shown in Fig. 5. Each projection displays a densely filled region rather than closed periodic orbits, highlighting the sensitive dependence on initial conditions and the system's aperiodic behavior. The x–y projection exhibits a two-scroll-like pattern, while the x–z and y–z projections illustrate the nonlinear stretching and folding mechanism that underpins chaotic attractors. These geometric structures reinforce the evidence from the time series that the proposed system generates complex and unpredictable dynamics.

Random Number Generator

The theory of nonlinear dynamical systems, which is the subfield of chaos theory emphasizes the importance in the field of randomness. Random number generation is an application of nonlinear dynamical systems. The chaotic behavior of the system determines the randomness and security of the generated random numbers.

After integrating the chaotic system numerically, the trajectories (x(t),y(t),z(t)) obtained from the solution were used as the basis for random number generation. An initial transient portion of the solution was discarded to eliminate settling effects, and the remaining data were sampled at fixed intervals with a decimation step to reduce short-term correlations. The sampled values were then converted into integers by scaling and normalizing their fractional parts. Finally, a mixing procedure based on bitwise operations, such as XOR and bit rotations, was applied to combine the contributions of x, y, and z. This post-processing step strengthens the statistical quality of the output, producing 32-bit random numbers suitable for evaluation with standard randomness test suites.

The importance of pseudo-random number generation in cryptographic systems is underscored by several NIST recommendations. The NIST SP800-22 test suite [47] provides widely adopted statistical procedures to evaluate the quality of random and pseudo-random sequences, serving as an essential first step in assessing cryptographic suitability. Complementing this, NIST SP800-90B [48] specifies design principles and validation tests for entropy sources, recommending a minimum of 1,000,000 samples to ensure meaningful statistical evaluation. Together with SP800-90A, which defines deterministic random bit generators, and SP800-90C, which describes how entropy sources and deterministic mechanisms can be combined, SP800-90B establishes a framework for robust random bit generation. Furthermore, NIST SP800-133 [49] highlights the central role of high quality randomness in cryptographic key generation, emphasizing that the unpredictability of keys is as critical as the strength of the algorithms themselves.

Several statistical tests can be used to evaluate the quality and applicability of pseudo-random number generators. In this study, we employed three well known test suites: the NIST Special Publication 800-22 suite provided by the National Institute of Standards and Technology (NIST) [41], the Diehard test [46], and the ENT test [50], with the corresponding results presented in Tables 2–5. The NIST suite includes 15 individual statistical tests. For the evaluation of the proposed generator, a dataset of 18,000,000 bytes was produced. In this context, each byte was treated as one output sample, resulting in a total of 18 million samples. According to the recommendations of NIST SP800-90B, a minimum of 1,000,000 samples is required for meaningful statistical assessment. Since the dataset used here significantly exceeds this threshold, the results obtained from the NIST, Diehard, and ENT test suites can be regarded as both reliable and representative. This extensive sample size therefore provides a strong basis for confirming the statistical characteristics and randomness suitability of the proposed generator.

Table 3: Results Of the NIST Test suite

Statistical Test	p-values	Proportion Of Passing Blocks
Frequency	0.173432	0.9862
Block Frequency	0.401509	0.78
Linear Complexity	0.148094	0.9833
Runs	0.092585	0.9833
FFT	0.183506	0.9862
ApEn	0.098189	0.9667
Serial	0.706149	0.9833
Cumulative-Sum	0.182801	0.9333
Logest Run	0.11511	0.9333
Rank	0.232760	0.9999
Universal	0.6	0.87837
Overlapping Templates	0.106242	0.9500
Non Overlapping Templates	0.257242	0.9833

Table 4: ENT Test Results

Test Name	Value	Result
Entropy	14.287712	Pass
Chi-square Statistic	14.774000	Pass
Chi-square p-value	0.097334	Pass
Mean	0.503333	Pass
Standard Deviation	0.289699	Pass
Serial Correlation	-0.002353	Pass
Monte Carlo Pi Estimate	3.102000	Pass

Table 5: Results relevant to NIST-Test suite

Statistical Test	X	p-values	Result
Random Excursion	X=-4	0.171169	SUCCESS
	X=-3	0.240286	SUCCESS
	X=-2	0.649849	SUCCESS
	X=-1	0.555839	SUCCESS
	X=1	0.568787	SUCCESS
	X=2	0.214818	SUCCESS
	X=3	0.186411	SUCCESS
	X=4	0.813536	SUCCESS
Random Excursion Variant	X=-9	0.797607	SUCCESS
	X=-8	0.815871	SUCCESS
	X=-7	0.869827	SUCCESS
	X=-6	0.807393	SUCCESS
	X=-5	0.975191	SUCCESS
	X=-4	0.943776	SUCCESS
	X=-3	0.540579	SUCCESS
	X=-2	0.332268	SUCCESS
	X=-1	0.950406	SUCCESS
	X=1	0.237307	SUCCESS
	X=2	0.222115	SUCCESS
	X=3	0.152003	SUCCESS
	X=4	0.295507	SUCCESS
	X=5	0.520417	SUCCESS
	X=6	0.606057	SUCCESS
	X=7	0.762743	SUCCESS
	X=8	0.772531	SUCCESS
	X=9	0.780189	SUCCESS

Table 6: Diehard Test Results

Test Name	p-value	Result
Diehard Birthdays	0.8569	Passed
Diehard Operm5	0.6597	Passed
Diehard Rank 32x32	0.4244	Passed
Diehard Rank 6x8	0.2376	Passed
Diehard Bitstream	0.9582	Passed
Diehard OPSO	0.9989	Weak
Diehard OQSO	0.6666	Passed
Diehard DNA	0.6596	Passed
Diehard Count 1s (stream)	0.3742	Passed
Diehard Count 1s (byte)	0.7106	Passed
Diehard Parking Lot	0.1530	Passed
Diehard 2D Sphere	0.4162	Passed
Diehard 3D Sphere	0.8110	Passed
Diehard Squeeze	0.5153	Passed
Diehard Sums	0.6208	Passed
Diehard Runs	0.9314	Passed
Diehard Runs (2nd)	0.5144	Passed
Diehard Craps	0.3592	Passed
Diehard Craps (2nd)	0.2310	Passed
Marsaglia Tsang GCD (1st)	0.1093	Passed
Marsaglia Tsang GCD (2nd)	0.7032	Passed
STS Monobit	0.4720	Passed
STS Runs	0.7791	Passed
STS Serial (30 tests)	0.1054 - 0.9907	All Passed
RGB Bitdist (10 tests)	0.0076 - 0.9295	All Passed
RGB Minimum Distance (4 tests)	0.3063 - 0.9787	All Passed
RGB Permutations (4 tests)	0.1502 - 0.9043	All Passed
RGB Lagged Sum (20 tests)	0.0254 - 0.9869	All Passed

The statistical quality of the proposed chaotic random number generator was evaluated using the NIST SP 800-22 test suite, the ENT package, and the Diehard battery of tests. As summarized in Table 3 and Table 5, the sequences successfully passed all NIST tests, with p-values distributed within the acceptable interval [0.01,0.99] and proportions of passing blocks consistently above the minimum thresholds. Although a few tests, such as Block-Frequency (0.78) and Universal (0.8737), exhibited slightly lower proportions, these values remain within the permissible range, confirming that the generated sequences do not display detectable bias. The ENT results (Table 4) further support this conclusion, showing near ideal statistical properties with an entropy value of 14.2877 (very close to the theoretical maximum of 14.28 for 8-bit data), a mean of 0.5033 (ideal 0.5), and a standard deviation of 0.2896 (expected 0.2887). The negligible serial correlation coefficient (−0.0023) demonstrates the independence of successive values, while the Monte Carlo estimation of π (3.1020) closely approximates the expected value of 3.1416. Finally, the results of the Diehard tests (Table 6) confirm the robustness of the generator, with all subtests passed and p-values distributed uniformly, thereby validating both short and long range randomness. Taken together, these results demonstrate that the proposed method reliably produces unbiased, statistically random sequences, supporting its suitability for cryptographic and stochastic applications.

Conclusion

In this study, a new quadratic Lorenz-like attractor was proposed and comprehensively analyzed as a foundation for pseudo-random number generation. A full dynamical investigation, including equilibrium analysis, Jacobian eigenvalues, bifurcation analysis, Lyapunov exponents, and fractional dimension, confirmed that the system possesses rich nonlinear dynamics and strong chaotic intensity induced by the quadratic coupling term. Numerical simulations, phase portraits, and bifurcation diagrams further demonstrated the transition from equilibrium states to oscillatory regimes and eventually to chaos as control parameters varied, thereby validating the system's suitability as a robust chaotic source.

Building on this foundation, pseudo-random sequences were extracted from the system and subjected to rigorous statistical validation using the NIST SP 800-22, Diehard, and ENT test suites. With a dataset of 18,000,000 bytes well above the minimum requirements specified by NIST SP 800-90B the proposed generator consistently passed all tests, achieving high entropy, uniform distribution, negligible correlation, and reliable long and short range randomness. These results confirm that the quadratic Lorenz-like attractor is not only mathematically

novel but also practically effective as a chaos based pseudo-random number generator suitable for cryptographic applications.

Overall, the research presented here demonstrates both the theoretical richness and the practical utility of the proposed system. By combining rigorous system analysis with statistical validation, this work establishes a strong foundation for future exploration of chaos driven security mechanisms. In particular, hardware implementation, benchmarking against alternative PRNGs, and deployment in real world secure communication frameworks will form important directions for extending the applicability of the proposed chaotic generator.

Conflicts of interest

There are no conflicts of interest in this work.

Ethical Approval Statement

There is no Ethical Approval needed for this work.

References

[1] Diffie W., Hellman M., New directions in cryptography, *IEEE Trans. Inf. Theory*, 22 (6) (1976) 644-654.

[2] Rivest R.L., Shamir A., Adleman L., A method for obtaining digital signatures and public-key cryptosystems, *Commun. ACM*, 21 (2) (1978) 120-126.

[3] Rivest R.L., Shamir A., Adleman L., A method for obtaining digital signatures and public-key cryptosystems, *Commun. ACM*, 26 (1) (1983) 96-99.

[4] Lin T., Chua L., A new class of pseudo-random number generator based on chaos in digital filters, *Int. J. Circuit Theory Appl.*, 21 (5) (1993) 473-480.

[5] Lücher M., A portable high-quality random number generator for lattice field theory simulations, *Comput. Phys. Commun.*, 79 (1) (1994) 100-110.

[6] Zhang S.C., Zhou S.M., A pseudo-random number generator, *Math. Practice Theory*, 1 (1992) 33-34.

[7] Bonilla L.L., Alvaro M., Carretero M., Chaos-based true random number generators, *J. Math. Ind.*, 7 (2017) 1-17.

[8] Teh J.S., Samsudin A., Al-Mazrooie M., Akhavan A., GPUs and chaos: a new true random number generator, *Nonlinear Dyn.*, 82 (4) (2015) 1913-1922.

[9] Avaroglu E., Koyuncu I., Ozer A.B., Turk M., Hybrid pseudo-random number generator for cryptographic systems, *Nonlinear Dyn.*, 82 (1-2) (2015) 239-248.

[10] Lynnyk V., Sakamoto N., Čelikovský S., Pseudo random number generator based on the generalized Lorenz chaotic system, *IFAC-Pap. OnLine*, 48 (18) (2015) 257-261.

[11] Cho K., Miyano T., Design and test of pseudorandom number generator using a star network of Lorenz oscillators, *Int. J. Bifurcation Chaos*, 27 (12) (2017) 1750184.

[12] Ebrahimzadeh R., Jampour M., Chaotic genetic algorithm based on Lorenz chaotic system for optimization problems, *Int. J. Intell. Syst. Appl.*, 5 (5) (2013) 19-24.

[13] Abdelhaleem S.H., Abd-El-Hafiz S.K., Radwan A.G., Analysis and guidelines for different designs of pseudo random number generators, *IEEE Access*, (2024).

[14] Zhao X.-Q., Dynamical systems in population biology, Springer, Berlin, (2013).

[15] Tél T., de Moura A., Grebogi C., Károlyi G., Chemical and biological activity in open flows: A dynamical system approach, *Phys. Rep.*, 413 (2) (2005) 91-196.

[16] Rössler O.E., Chaos and chemistry. In: Nonlinear phenomena in chemical dynamics, Springer, Berlin, (1981) 79-87.

[17] Rössler O.E., An equation for continuous chaos, *Phys. Lett. A*, 57 (5) (1976) 397-398.

[18] Lorenz E.N., Deterministic nonperiodic flow, *J. Atmos. Sci.*, 20 (2) (1963) 130-143.

[19] Arnold V.I., Mathematical methods of classical mechanics, Springer, Berlin, (1989).

[20] Kyrtsou C., Labys W.C., Evidence for chaotic dependence between US inflation and commodity prices, *J. Macroecon.*, 28 (1) (2006) 256-266.

[21] Kyrtsou C., Vorlow C.E., Complex dynamics in macroeconomics: A novel approach. In: New trends in macroeconomics, Springer, Berlin, (2005) 223-238.

[22] Peters E.E., Fractal market analysis: applying chaos theory to investment and economics, John Wiley & Sons, New York, (1994).

[23] Poincaré H., Sur le problème des trois corps et les équations de la dynamique, *Acta Math.*, 13 (1) (1890) A3-A270.

[24] Fatou P., Sur les substitutions rationnelles, *C. R. Acad. Sci. Paris*, 164 (1917) 806-808.

[25] Julia G., Mémoire sur l'itération des fonctions rationnelles, *J. Math. Pures Appl.*, 1 (1918) 47-246.

[26] Birkhoff G.D., On the periodic motions of dynamical systems, *Acta Math.*, 50 (1) (1927) 359-379.

[27] Kolmogorov A.N., The local structure of turbulence in incompressible viscous fluid for very large Reynolds numbers, *Dokl. Akad. Nauk SSSR*, 30 (1941) 299-303.

[28] Kolmogorov A.N., Preservation of conditionally periodic movements with small change in the Hamilton function. In: Casati G., Ford J., (Eds.), Stochastic behavior in classical and quantum Hamiltonian systems, Lecture Notes in Physics, Vol. 93, Springer, Berlin, (1979) 51-56.

[29] Kolmogorov A.N., Dissipation of energy in the locally isotropic turbulence, *Proc. R. Soc. Lond. A*, 434 (1991) 15-17.

[30] Cartwright M., Littlewood J., On non-linear differential equations of the second order: II. The equation y+kf(y,y+g(y,k)=p(t)=p1(t)+kp2(t); k>0, f(y)≠1, *Ann. Math.*, (1947) 472-494.

[31] Smale S., Morse inequalities for a dynamical system, *Bull. Am. Math. Soc.*, 66 (1) (1960) 43-49.

[32] Smale S., On gradient dynamical systems, *Ann. Math.*, (1961) 199-206.

[33] Shaw R., Strange attractors, chaotic behavior and information flow, *Z. Naturforsch. A*, 36 (1981) 80-112.

[34] Chen G., Ueta T., Yet another chaotic attractor, *Int. J. Bifurcation Chaos*, 9 (7) (1999) 1465-1466.

[35] Lü J., Chen G., A new chaotic attractor coined, *Int. J. Bifurcation Chaos*, 12 (3) (2002) 659-661.

[36] Yang Q., Wei Z., Chen G., An unusual 3D autonomous quadratic chaotic system with two stable node-foci, *Int. J. Bifurcation Chaos*, 20 (4) (2010) 1061-1083.

[37] Pehlivan I., Uyaroğlu Y., A new chaotic attractor from general Lorenz system family and its electronic experimental implementation, *Turk. J. Electr. Eng. Comput. Sci.*, 18 (2) (2010) 171-184.
[38] Cuomo K.M., Oppenheim A.V., Circuit implementation of synchronized chaos with applications to communications, *Phys. Rev. Lett.*, 71 (1) (1993) 65-68.
[39] Yu S., Lü J., Tang W.K., Chen G., A general multiscroll Lorenz system family and its realization via digital signal processors, *Chaos*, 16 (3) (2006) 033126.
[40] Lü J.G., Chaotic dynamics of the fractional-order Lü system and its synchronization, *Phys. Lett. A*, 354 (4) (2006) 305-311.
[41] Bassham L.E., Rukhin A.L., Soto J., Nechvatal J.R., Smid M.E., Barker E.B., et al., A statistical test suite for random and pseudorandom number generators for cryptographic applications, NIST Special Publication 800-22 Rev. 1a, NIST, Gaithersburg, (2010).
[42] Hahn W., Baartz A.P., Stability of motion, Springer, Berlin, (1967).
[43] Argyris J., Faust G., Haase M., Friedrich R., An exploration of dynamical systems and chaos, 2nd ed., Springer, Berlin, (2015).
[44] Kaplan J.L., Yorke J.A., Chaotic behavior of multidimensional difference equations. In: Functional differential equations and approximation of fixed points, Springer, Berlin, (1979) 204-227.
[45] Chlouverakis K.E., Sprott J., A comparison of correlation and Lyapunov dimensions, *Physica D*, 200 (1-2) (2005) 156-165.
[46] Brown R.G., Eddelbuettel D., Bauer D., Dieharder, Duke University Physics Department, Durham, NC, (2018).
[47] Bassham L.E., Rukhin A.L., Soto J., Nechvatal J.R., Smid M.E., Leigh S.D., et al., A statistical test suite for random and pseudorandom number generators for cryptographic applications, NIST SP 800-22 Rev. 1a, NIST, Gaithersburg, (2010).
[48] Turan M.S., Barker E., Kelsey J., McKay K., Baish M., Boyle M., Recommendation for the entropy sources used for random bit generation, NIST Special Publication 800-90B (Draft), NIST, Gaithersburg, (2016).
[49] Barker E., Roginsky A., Davis R., Recommendation for cryptographic key generation, NIST Special Publication 800-133 Rev. 1, NIST, Gaithersburg, (2012).
[50] Walker J., ENT: a pseudorandom number sequence test program. Available at: http://www.fourmilab.ch/random/. Retrieved March 2, 2008.