# NIST Test Validation for Lorenz Chaotic Random Generator CRN

Amr Sayed AbdelFattah Youssef

***Abstract*— The necessity of developing a secure communication system that safeguards privacy and sensitive data against hacker attacks and eavesdroppers is now widely acknowledged. This necessitates the creation of solutions that not only deal with security issues but also shouldn't slow down our system. Most security systems rely on randomness generators to establish safe communication; more randomness equals more security. Random generators are essential to the encryption process. In this research, a design and implementation process for a novel random generator based upon Lorenz chaotic signals is presented. NIST's Statistical Test Suite for Random and Pseudorandom Generators for Cryptographic Applications has been used to evaluate the proposed chaotic random generator CRN, and the findings have been reviewed.**

***Index Terms*— Chaotic random generator, NIST, Randomness, security, wireless**

## I. Introduction

Chaotic signals possess several characteristics that render them appealing for communication systems. Firstly, their wideband nature allows them to withstand the negative impacts of multipath fading. As a result, when these signals are employed to encode information, they generate spread-spectrum signals with broader bandwidth and reduced power spectral densities. In addition, chaotic signals can generate a multitude of spreading waveforms with ease because of their sensitivity to initial conditions. Furthermore, they have a rather uniform frequency spectrum because of their nonperiodic character in the time domain. They are also suitable for secure communication because of their noise-like signal structure, which offers a high level of secrecy and has a minimal likelihood of being detected and intercepted. Additionally, the synchronization of chaotic systems is theoretically and practically possible [1]-[4].

The primary attribute of this signal type lies in its ability to be effortlessly generated by uncomplicated circuits, enabling the cost-effective implementation of the product. Considering all the aforementioned properties, chaotic signals are an ideal candidate for use in secure communication systems [4]. The security aspects of chaos-based cryptosystems have been studied in several works [5],[6].

[7],[8] demonstrated the feasibility of unmasking certain chaos-based secure communication systems by modeling and predicting the transmitter. Moreover, a recent analysis of the receiver parameters in a chaos-based cryptosystem, employing chaotic synchronization, indicated that the system's security is vulnerable to specific attacks when the dynamic model of the chaos system is known [9],[10].

Our main objective is to develop a chaotic cryptosystem that achieves "provable security," indicating that mathematical proofs demonstrate its ability to withstand specific types of attacks. C.E. Shannon conducted groundbreaking research in this domain. In his information theory, he formulated measures for quantifying the information contained within a message and introduced the concept of perfect secrecy: a perfectly secret cipher perfectly resists all ciphertext-only attacks. An adversary gets no information about the plaintext, even if his computing power and time resources are unlimited [11].

Shannon's perfect secrecy can be summarized in the following statement [11]: "An encryption is perfectly secret if and only if an adversary cannot distinguish between two plaintexts, even if his computing resources are unlimited". For instance, if the adversary possesses the knowledge that a ciphertext "*c*" corresponds to the encryption of either "1" or "0", their probability of correctly selecting the correct option is no greater than 1/2. This probability can be obtained even without knowing the ciphertext. In other words, the reception of ciphertext doesn't improve the vision of the adversary or increase the probability of any specific plaintext over others. Consequently, there is a strong interconnection between randomness and the security of cryptographic schemes. Without randomness, security cannot be achieved. An encryption method provides secrecy only if the ciphertexts appear random to the adversary [1].

The most renowned cipher that achieves perfect secrecy is Vernam's one-time pad. This cipher encrypts a message "m" by performing a bitwise XOR operation with a genuinely random bit string. It successfully withstands all passive attacks and can be mathematically proven to be secure using Shannon's theory [12]. The one-time pad is considered perfectly secret because the resulting bit sequence "*c(t)*" obtained by XORing the encrypted message "*m(t)*" with the truly random key string "*k(t)*" appears entirely random to any potential adversary. Fig. 1 shows Vernam's one-time pad or XORing encryption technique.

Random number generators serve practical purposes in diverse fields, as emphasized in [13]:

- Cryptography and image watermarking to ensure image authentication.
- Generating message keys for ciphers.
- Creating random challenges for authentication purposes.
- Generating passwords.

Manuscript received April 03, 2023; revised September 04, 2023.

Amr S. Youssef is an Associate Professor in Higher Colleges of Technology HCT in UAE (ayoussef@hct.ac.ae).

- Facilitating secure communication.
- Enabling simulation, such as Monte Carlo simulation.
- Serving as initialization vectors for neural networks and genetic algorithms.
- Simulating noise for evaluating communication systems.

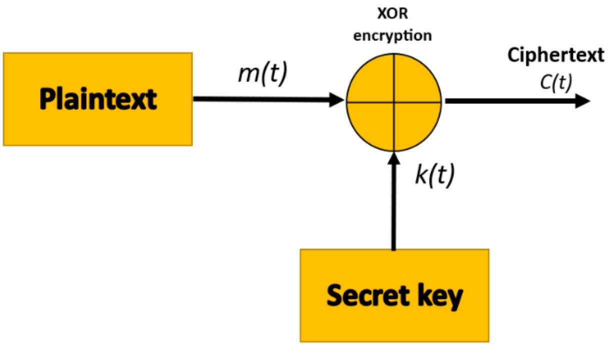

Fig. 1. Vernam's One-Time Pad Or XORing Encryption Technique

An RNG (Random Number Generator), whether computational or physical, is a device specifically created to produce a sequence of numbers or symbols that exhibit no discernible pattern, thus appearing random. While computer-based RNG systems are commonly employed, they often fall short of achieving true randomness. However, they may satisfy certain statistical tests for randomness, which aim to confirm the absence of easily identifiable patterns. [11]

Let us suppose that the set of possible messages is finite in number $m_1, \ldots, m_n$ that these have a priori probabilities $P(m_1), \ldots , P(m_n)$, and that messages are enciphered into possible cryptograms $E_1, \ldots, E_m$ by

$$E = k_i m \tag{1}$$

When a cryptanalyst intercepts a specific ciphertext "*E*," they can compute the posterior probabilities, denoted as $P_E(m)$, for different possible messages. Perfect secrecy is naturally defined by the condition where, for any ciphertext "*E*" the posterior probabilities are equal to the prior probabilities. In such a scenario, intercepting the message provides the cryptanalyst with no additional information. A necessary and sufficient condition for perfect secrecy can be found as follows in the Bayes' theorem [14]

$$P_E(m) = \frac{P(m)P_m(E)}{P(E)} \tag{2}$$

where

$P(m)$ is the a priori probability of message *m*.

$P_m(E)$ is the conditional probability of cryptogram *E* if message m is chosen, i.e. the sum of the probabilities of all the keys which produce cryptogram *E* from message *m*.

$P(E)$ is the probability of obtaining cryptogram *E* from any cause.

$P_E(m)$ a posteriori probability of message *m* if cryptogram *E* is intercepted.

For perfect secrecy, $P_E(m)$ must equal $P(m)$ for all *E* and for all *m*. For our proposed system, the data to be transmitted is binary "0" or "1" with equal probability, $P(0)=P(1)=P(m)=1/2$. Because this data is encrypted by a random key to produce E, the randomness leads us to say that $P_m(E)=P(E)=1/2$. Therefore, it is obvious that the condition of perfect security is satisfied in our system, where $P_E(m)$ equals $P(m)$.

The primary obstacle lies in generating and managing sufficiently long truly random bit sequences, which is often impractical to achieve for perfect secrecy in many cases. To address this issue, we propose employing a chaotic random number generator for generating the secret key. The randomness of the utilized key has been validated through the NIST test [15]. By utilizing the XORing technique with the proven randomness of the key, we can attain perfect security.

## II. RANDOMNESS CHARACTERISTICS OF THE CHAOTIC SIGNAL

In the suggested CRNG, the parameters of the chaotic signal act as random seeds, and the running-key sequence can be generated from the binary variables produced by the chaotic dynamics. The new approach relies on frequency-domain aliasing to improve the randomness of the running-key sequence and improve the security of the key seeds. Aliasing in the frequency domain is achieved by sampling the chaotic signal at a frequency within its bandwidth. This results in a flatter and whiter frequency spectrum of the sampled discrete-time sequence, which enhances randomness. Moreover, the running-key sequence derived from the sampled chaotic signal is highly sensitive to the sampling frequency. The enhanced security of the cryptosystem can be attributed to the heightened randomness of the running-key sequence and the nonanalytical characteristics of the sampling frequency. The randomness of the running-key sequence and its sensitivity to the sampling frequency are quantitatively evaluated by the correlation functions. In the realm of stream cipher cryptography, an important challenge is the efficient generation of a lengthy running-key sequence from short and random keys, also known as key seeds [16]. In chaos-based cryptosystems, the random seeds are denoted by the parameters and initial conditions of the chaos systems, while the running-key sequences are derived from the sampled state variables of the system obtained through chaotic dynamics. Due to the sensitivity of chaotic systems to both initial conditions and parameter changes, certain chaotic systems offer a sufficiently large parameter space to accommodate random key seeds. The running-key sequence can be recovered from the receiver side by synchronization of the chaotic systems [2]-[4]. In order to enhance the randomness of the operational key sequence, a sampling method for the continuous-time chaotic signal is showcased, employing a sampling frequency significantly lower than the chaotic signal's bandwidth. Since the spectrum of the sampled discrete-time sequence can be flattened due to frequency-domain aliasing, its degree of randomness can be increased by slowing down the sampling frequency. Thus, the sampled discrete-time sequence as the running-key sequence and the sampling frequency can be used together with the chaotic system parameters as the key seeds.

The Simulink model for the sample Lorenz chaotic signal is depicted in Fig. 2. The Lorenz system, which comprises three interconnected first-order ordinary differential equations as outlined in equations 4-6, is utilized in this model.

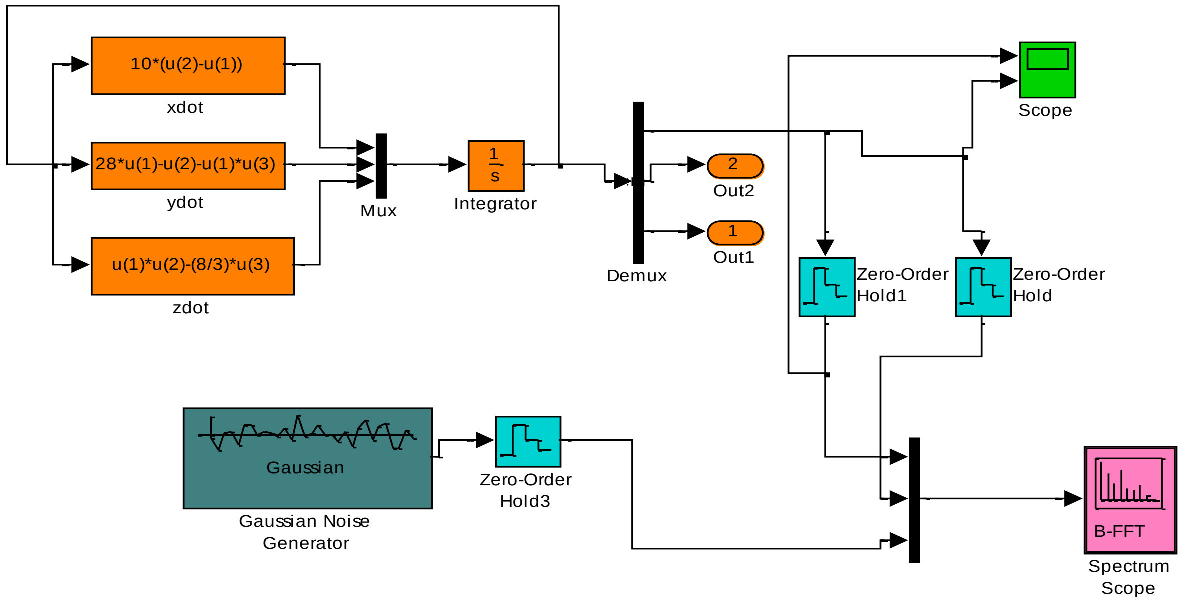

Fig. 2. Simulink model for sampling Lorenz chaotic signal

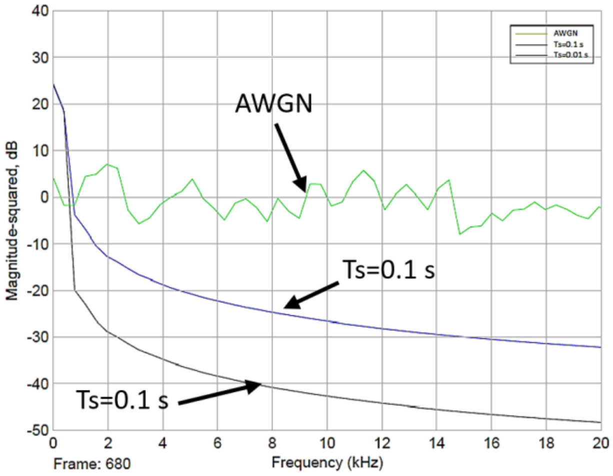

Fig. 3. Frequency spectra of xs with different sampling periods.

$$\frac{du}{dt} = K(c_1 v - c_1 u) \tag{4}$$

$$\frac{dv}{dt} = K(c_2 u - v - uw) \tag{5}$$

$$\frac{dw}{dt} = K(uv - c_3 w) \tag{6}$$

where $c_1$ , $c_2$ and $c_3$ are arbitrary constants with the values 10, 28, and 2.666 respectively. *K* represents the time scaling factor of the Lorenz system [17]. The frequency spectra of the sampling periods are shown in Fig. 3, where $T_s$=0.1, 0.01 sec, and the spectra of AWGN is added for comparison purpose.

There are several reasons to support the notion that utilizing sampled chaotic sequences with frequency domain aliasing can significantly enhance the secure protection of a cryptosystem against attacks. Firstly, the sampled running-key sequence is highly sensitive to the non-analytical nature of the sampling frequency. This sensitivity improves the security of the key seeds when the sampling frequency is incorporated into them. Consequently, there is no information regarding the original sampling rate of the running-key sequence contained in the encrypted data sequence transmitted through the communication channel.

Secondly, frequency aliasing renders it impossible to reconstruct the original continuous-time chaotic signal from the running-key sequence.

Lastly, the running-key sequence with frequency domain aliasing provides minimal information for directly estimating the parameters of the continuous-time chaotic systems. In contrast, recent research has demonstrated that using only the continuous-time chaotic signal makes the cryptosystem vulnerable to certain attacks. [18,19,20].

## III. CHAOTIC RANDOM NUMBER GENERATOR (CRNG)

The schematic diagram for the proposed chaotic random number generator (CRNG) is shown in Fig. 4. As shown in the Figure, the chaotic signal is sampled at regular intervals using a sample and hold circuit. The sampled signal is mapped into either “0” or “1” by a decision circuit and then the output is fed to a buffer register. Finally, the randomness of the generated sequences is assessed by the NIST test suites.

Statistical tests evaluate the randomness of a bit sequence by analyzing its probability characteristics. The NIST Suite and the Diehard Suite are widely regarded as the most rigorous statistical tests for assessing randomness among all internationally recognized tests. They both include dozens of independent and computationally intensive statistical tests. Most of these tests return a test statistic and its corresponding probability value (p-value) [15]. The p-value is the probability of obtaining a test statistic as “impressive” as the one observed if the sequence is random so that the statistic was the result of chance alone. In other words, the p-value summarizes the strength of the evidence against the perfect randomness hypothesis. Small values (p-values < 0.01) are interpreted as evidence that a sequence is unlikely to be random. Here 0.01 is the significance level, usually denoted as α.

The NIST Suite [15] provides a battery of 16 statistical tests. They assess the presence of a pattern which, if detected,

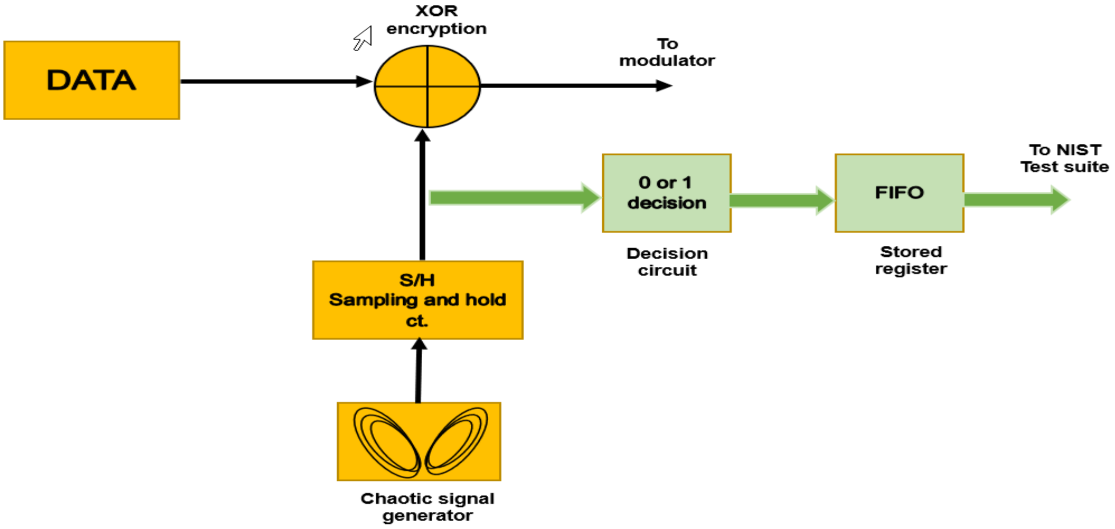

Fig. 4. Schematic Diagram for Chaotic Random Number Generator (CRNG)

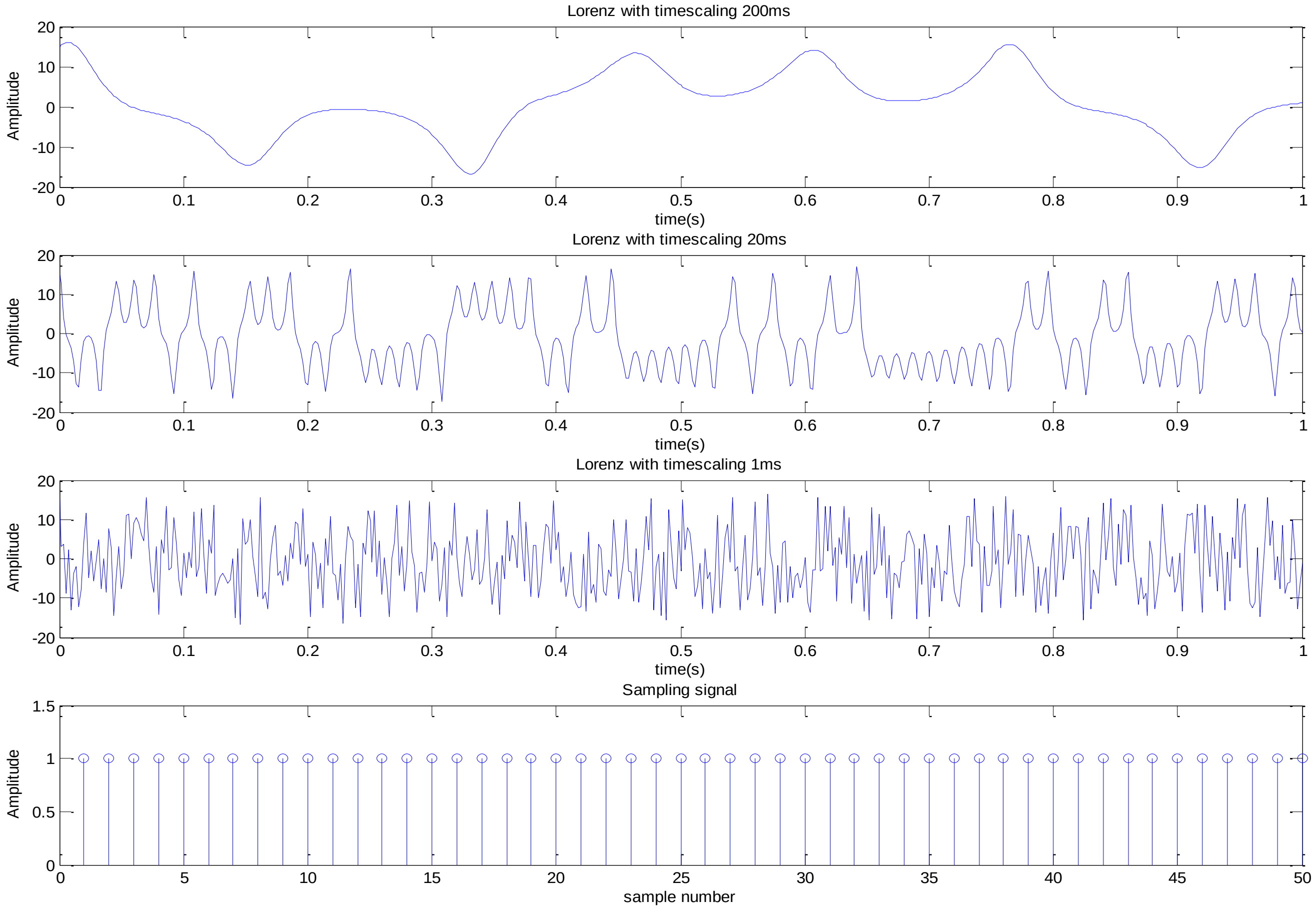

Fig. 5. u-Lorenz chaotic signal with different time scaling versus sampling frequency (a) u-Lorenz signal with time scaling equals 200 ms (b) u-Lorenz signal with time scaling equals 20 ms (c) u-Lorenz signal with time scaling equals 1 ms (d) sampling signal.

would indicate that the sequence is non-random. In each test, a p-value is calculated. The significance level α for all tests in the NIST Suite is set to 1%. A p-value of zero indicates that the sequence appears to be completely non-random. A p-value less than α would mean that the sequence is non-random with a confidence of 99%. If a p-value is greater than α, the sequence is random with a confidence of 99%.

## IV. NUMERICAL ANALYSIS

In the following section, NIST test results for a CRNG like that shown in Fig. 4 are demonstrated. where the chaotic source is represented by the Lorenz oscillator. The sampling should be done at a frequency much less than the fundamental frequency of the chaotic oscillator ($f_{sampling}$<<$f_{fundamental}$). The fundamental frequency is determined by the reciprocal of the time taken for one complete rotation around a chaotic attractor. This implies that the variation in the chaotic signal between two consecutive samples is significant enough to enhance the randomness processing and fulfill the requirements of the frequency aliasing technique. Fig. 5

(a),(b),(c) represent the Lorenz u-signal with time scaling 200 *ms*, 20 *ms*, and 1 *ms* respectively, and Fig. 5.(d) represents the sampling signal that will apply for all cases and its value is supposed to be constant and equals 50 Hz for all three cases. As shown in Fig. 5(c), in the case of high-time scaling of 1 *ms*, the u-signal appears to exhibit characteristics of a noise signal in relation to the sampling signal. Consequently, it is expected that the randomness, in this case, would be higher compared to the other two cases.

Fig. 6 shows the Simulink model used in numerical analysis. The time scaling for three Lorenz differential equations is 250 µs and the initial conditions for u, v, and w are taken as 15, 20, and 30 respectively. The numerical results of P-values for the 16 statistical tests conducted by NIST are presented in Tables I to VII, showcasing the outcomes for various combinations of Lorenz time scaling and sampling frequencies.

## V. SIMULATION RESULTS

Tables I and II demonstrate that when the sampling frequency (50 kHz) and time scaling (1 *ms* and 400 µs) fall short, they do not offer any degree of randomness, resulting in failure across all NIST tests.

The outcomes presented in Table III indicate that when using a sampling frequency of 50 kHz and time scaling of 250 µs, a noticeable level of randomness is achieved. Nearly half of the NIST tests are successfully passed.

The data presented in Table IV reveals that when the time scaling is held at 250 µs and the sampling frequency is reduced to 20 kHz, a certain level of randomness begins to emerge. In this case, two tests are successfully passed. Conversely, when the time scaling is reduced to just 25 µs while maintaining a sampling frequency of 20 kHz, the level of randomness intensifies, resulting in the successful passing of 8 out of 16 tests, as indicated in Table V.

Displayed in Table VI are the outcomes obtained by decreasing the time scaling to 16.667 µs and applying a sampling frequency of 20 kHz. The results reveal the successful passing of the majority of tests (11 out of 16), while the remaining two tests are unable to be finalized due to an insufficient number of cycles.

By decreasing the sampling frequency to only 500 Hz while maintaining a time scaling of 250 µs, all tests are successfully passed, resulting in the attainment of randomness, as shown in Table VII.

## VI. CONCLUSIONS

This research paper aimed to address a prevalent issue involving the generation of true random numbers. This issue holds significant implications for various industries that depend on random number generation, spanning from credit card companies and secure communication to lotteries. The concern stems from the potential vulnerability if an attacker manages to predict the underlying mechanism of the randomness generation, enabling them to exploit it. Regrettably, the process of generating authentic random numbers appears deceptively simple compared to its actual complexity. In essence, achieving truly random numbers through any deterministic device is fundamentally unfeasible.

This work tries to find an alternative way of thinking to produce a randomness number that diverges significantly from conventional approaches reliant on pseudo-random number generators (PRNGs), which follow predictable patterns through mathematical formulas, or from the utilization of quantum processes.

The simulation tests demonstrate that the suggested CRNG produces a highly unpredictable final number, which makes it suitable for most practical purposes requiring randomness.

Through simulation, this study conclusively demonstrates that the randomness of the Cryptographically Secure Random Number Generator (CRNG) is primarily governed by two key factors: the sampling frequency and the time scaling of the Lorenz generator. The previous NIST test results affirm the presence of a trade-off process associated with these factors. This compromise entails two distinct cases:

The first case involves maintaining a consistent sampling frequency while reducing the scaling time, resulting in an augmentation of the randomness characteristics of the generated bits.

The second case involves maintaining a constant scaling

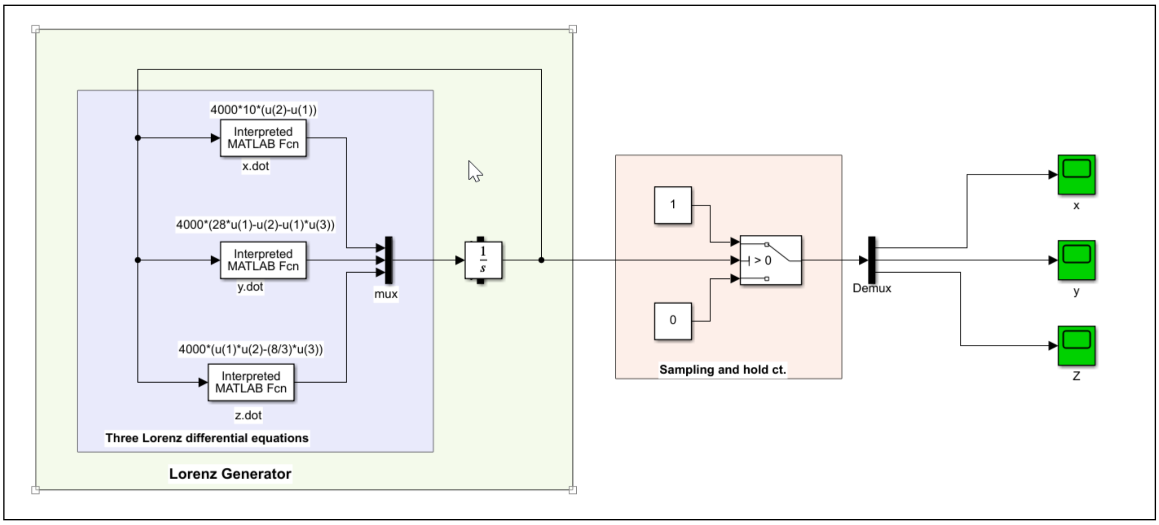

Fig. 6. Simulink® simulation for Lorenz CRNG used in the analysis

time while decreasing the sampling frequency, leading to an improvement in the randomness properties of the generated bits. However, it is worth noting that in either scenario, the computation simulation time will increase. In the first case, the simulation steps must be increased to accurately capture the rapid variation of the Lorenz signal. In the second case, the simulation time for our model needs to be extended to generate the same number of bits before reducing the sampling frequency.

Throughout our analysis, several noteworthy points have been deduced, including:

1- Choosing a stream cipher for encryption, utilizing its beneficial attributes like rapid encryption/decryption operations. This choice aligns with the design objective of a high-speed transmission system with real-time applications. Additionally, the implementation can be accomplished using a straightforward circuit like XOR.

2- Applying the sampling theory to chaotic signals to devise a genuine Cryptographically Secure Random Number Generator (CRNG). At the same time, the concept of frequency aliasing presents considerable obstacles in the process of reconstructing the initial continuous-time chaotic signal from the operational key sequence.

TABLE I
NIST results for Lorenz with time scaling 1 ms and sampling $F_{SAMPLING}$=50 kHz

| Test ID | | *u* | *v* |
|---|---|---|---|
| **Frequency (monobit) test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Frequency Test within a Block** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Runs Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Test for the Longest Run of Ones in a Block** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Binary Matrix Rank Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Discrete Fourier Transform (Spectral) Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Non-overlapping Template Matching Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Overlapping Template Matching Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Maurer's "Universal Statistical" Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Linear Complexity Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Serial Test** | P_value1 | 0.0 | 0.0 |
| | P_value2 | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Approximate Entropy Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Cumulative Sums forward Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Cumulative Sums Reverse Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Random Excursions Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Random Excursions Variant Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |

TABLE II
NIST results for Lorenz with time scaling 400 μs and sampling $F_{SAMPLING}$ =50 kHz

| Test ID | | *u* | *v* |
|---|---|---|---|
| **Frequency (monobit) test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Frequency Test within a Block** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Runs Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Test for the Longest Run of Ones in a Block** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Binary Matrix Rank Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Discrete Fourier Transform (Spectral) Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Non-overlapping Template Matching Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Overlapping Template Matching Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Maurer's "Universal Statistical" Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Linear Complexity Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Serial Test** | P_value1 | 0.0 | 0.0 |
| | P_value2 | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Approximate Entropy Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Cumulative Sums forward Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Cumulative Sums Reverse Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Random Excursions Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Random Excursions Variant Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |

TABLE III
NIST results for Lorenz with time scaling 250 μs and sampling $F_{SAMPLING}$=50 kHz

| Test ID | | *u* | *v* |
|---|---|---|---|
| **Frequency (monobit) test** | P_value | 0.257214 | 0.459300 |
| | status | PASS | PASS |
| **Frequency Test within a Block** | P_value | 0.044656 | 0.098090 |
| | status | PASS | PASS |
| **Runs Test** | P_value | 0.455496 | 0.749383 |
| | status | PASS | PASS |
| **Test for the Longest Run of Ones in a Block** | P_value | 0.271688 | 0.371372 |
| | status | PASS | PASS |
| **Binary Matrix Rank Test** | P_value | 0.480366 | 0.233657 |
| | status | PASS | PASS |
| **Discrete Fourier Transform (Spectral) Test** | P_value | 0.000000 | 0.000000 |
| | status | Failure | Failure |
| **Non-overlapping Template Matching Test** | P_value | 0.000000 | 0.000000 |
| | status | Failure | Failure |
| **Overlapping Template Matching Test** | P_value | 0.000000 | 0.000000 |
| | status | Failure | Failure |
| **Maurer's "Universal Statistical" Test** | P_value | 0.000000 | 0.000000 |
| | status | Failure | Failure |
| **Linear Complexity Test** | P_value | 0.958956 | 0.224222 |
| | status | PASS | PASS |
| **Serial Test** | P_value1 | 0.000000 | 0.000000 |
| | P_value2 | 0.000000 | 0.000000 |
| | status | Failure | Failure |
| **Approximate Entropy Test** | P_value | 0.000000 | 0.000000 |
| | status | Failure | Failure |
| **Cumulative Sums forward Test** | P_value | 0.041007 | 0.010509 |
| | status | PASS | PASS |
| **Cumulative Sums Reverse Test** | P_value | 0.000403 | 0.000587 |
| | status | Failure | Failure |
| **Random Excursions Test** | P_value | 0.000000 | 0.000000 |
| | status | Failure | Failure |
| **Random Excursions Variant Test** | P_value | 0.000000 | 0.000000 |
| | status | Failure | Failure |

Table IV
NIST results for Lorenz with time scaling 250 μs and sampling $F_{SAMPLING}$ =20 kHz

| Test ID | | *u* | *v* |
|---|---|---|---|
| **Frequency (monobit) test** | P_value | 0.3856 | 0.3399 |
| | status | PASS | PASS |
| **Frequency Test within a Block** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Runs Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Test for the Longest Run of Ones in a Block** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Binary Matrix Rank Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Discrete Fourier Transform (Spectral) Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Non-overlapping Template Matching Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Overlapping Template Matching Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Maurer's "Universal Statistical" Test** | P_value | 0.0 | 0.0 |
| | status | Failure | Failure |
| **Linear Complexity Test** | P_value | 0.6486 | 0.4196 |
| | status | PASS | PASS |
| **Serial Test** | P_value1 | 0 | 0 |
| | P_value2 | 0 | 0 |
| | status | Failure | Failure |
| **Approximate Entropy Test** | P_value | 0 | 0 |
| | status | Failure | Failure |
| **Cumulative Sums forward Test** | P_value | 0.0013 | 8.40e-004 |
| | status | Failure | Failure |
| **Cumulative Sums Reverse Test** | P_value | 0.0042 | 0.0041 |
| | status | Failure | Failure |
| **Random Excursions Test**<br>* Insufficient number of cycles to complete the test (considered fail). | P_value | * | * |
| | status | Failure | Failure |
| **Random Excursions Variant Test**<br>* Insufficient number of cycles to complete the test (considered fail). | P_value | * | * |
| | status | Failure | Failure |

Table V
NIST results for Lorenz with time scaling 25 μs and sampling $F_{SAMPLING}$ =20 kHz

| Test ID | | *u* | *v* |
|---|---|---|---|
| **Frequency (monobit) test** | P_value | 0.162714 | 0.649829 |
| | status | PASS | PASS |
| **Frequency Test within a Block** | P_value | 0.000078 | 0 |
| | status | Failure | Failure |
| **Runs Test** | P_value | 0 | 0 |
| | status | Failure | Failure |
| **Test for the Longest Run of Ones in a Block** | P_value | 0.532683 | 0.001174 |
| | status | PASS | Failure |
| **Binary Matrix Rank Test** | P_value | 0.233986 | 0.348678 |
| | status | PASS | PASS |
| **Discrete Fourier Transform (Spectral)** | P_value | 0.457296 | 0.440804 |
| | status | PASS | PASS |
| **Non-overlapping Template Matching Test** | P_value | 0.1294 | 0.0397 |
| | status | PASS | PASS |
| **Overlapping Template Matching Test** | P_value | 0 | 0 |
| | status | Failure | Failure |
| **Maurer's "Universal Statistical" Test** | P_value | 0.009265 | 0.000271 |
| | status | Failure | Failure |
| **Linear Complexity Test** | P_value | 0.762675 | 0.407226 |
| | status | PASS | PASS |
| **Serial Test** | P_value1 | 0.002504 | 0 |
| | P_value2 | 0.931594 | 0.046910 |
| | status | Partial PASS | Partial PASS |
| **Approximate Entropy Test** | P_value | 0 | 0 |
| | status | Failure | Failure |
| **Cumulative Sums forward Test** | P_value | 0.266181 | 0.915089 |
| | status | PASS | PASS |
| **Cumulative Sums Reverse Test** | P_value | 0.110476 | 0.516382 |
| | status | PASS | PASS |
| **Random Excursions Test** | P_value | 0.4488 | 0.4549 |
| | status | PASS | PASS |
| **Random Excursions Variant Test** | P_value | 0.7325 | 0.5215 |
| | status | PASS | PASS |

Table VI
NIST Results for Lorenz with Time Scaling 16.667 μs and Sampling $F_{SAMPLING}$ =20 kHz

| Test ID | | *u* | *v* |
|---|---|---|---|
| **Frequency (monobit) test** | P_value | 0.485177 | 0.353408 |
| | status | PASS | PASS |
| **Frequency Test within a Block** | P_value | 0.000354 | 0.000955 |
| | status | Failure | Failure |
| **Runs Test** | P_value | 0 | 0 |
| | status | Failure | Failure |
| **Test for the Longest Run of Ones in a Block** | P_value | 0.730426 | 0.256572 |
| | status | PASS | PASS |
| **Binary Matrix Rank Test** | P_value | 0.441499 | 0.197806 |
| | status | PASS | PASS |
| **Discrete Fourier Transform (Spectral) Test** | P_value | 0.514698 | 0.526611 |
| | status | PASS | PASS |
| **Non-overlapping Template Matching Test** | P_value | 0.2649 | 0.3207 |
| | status | PASS | PASS |
| **Overlapping Template Matching Test** | P_value | 0.048116 | 0.019115 |
| | status | PASS | PASS |
| **Maurer's "Universal Statistical" Test** | P_value | 0.143473 | 0.810594 |
| | status | PASS | PASS |
| **Linear Complexity Test** | P_value | 0.712669 | 0.819432 |
| | status | PASS | PASS |
| **Serial Test** | P_value1 | 0.077330 | 0.004559 |
| | P_value2 | 0.486258 | 0.270332 |
| | status | PASS | Partial PASS |
| **Approximate Entropy Test** | P_value | 0 | 0 |
| | status | Failure | Failure |
| **Cumulative Sums forward Test** | P_value | 0.763576 | 0.206624 |
| | status | PASS | PASS |
| **Cumulative Sums Reverse Test** | P_value | 0.712989 | 0.682964 |
| | status | PASS | PASS |
| **Random Excursions Test**<br>* Insufficient number of cycles to complete the test (considered fail). | P_value | 0.4492 | * |
| | status | PASS | Failure |
| **Random Excursions Variant Test**<br>* Insufficient number of cycles to complete the test (considered fail). | P_value | 0.5313 | * |
| | status | PASS | Failure |

Table VII
NIST results for Lorenz with time scaling 250 μs and sampling $F_{SAMPLING}$=500 Hz

| Test ID | | *u* | *v* |
|---|---|---|---|
| **Frequency (monobit) test** | P_value | 0.257214 | 0.459300 |
| | status | PASS | PASS |
| **Frequency Test within a Block** | P_value | 0.044656 | 0.098090 |
| | status | PASS | PASS |
| **Runs Test** | P_value | 0.455496 | 0.749383 |
| | status | PASS | PASS |
| **Test for the Longest Run of Ones in a Block** | P_value | 0.271688 | 0.371372 |
| | status | PASS | PASS |
| **Binary Matrix Rank Test** | P_value | 0.480366 | 0.233657 |
| | status | PASS | PASS |
| **Discrete Fourier Transform (Spectral) Test** | P_value | 0.578611 | 0.890517 |
| | status | PASS | PASS |
| **Non-overlapping Template Matching Test** | P_value (mean) | 0.5134 | 0.5293 |
| | status | PASS | PASS |
| **Overlapping Template Matching Test** | P_value | 0.301860 | 0.049567 |
| | status | PASS | PASS |
| **Maurer's "Universal Statistical" Test** | P_value | 0.306558 | 0.202464 |
| | status | PASS | PASS |
| **Linear Complexity Test** | P_value | 0.049207 | 0.354250 |
| | status | PASS | PASS |
| **Serial Test** | P_value1 | 0.737745 | 0.504885 |
| | P_value2 | 0.724442 | 0.351622 |
| | status | PASS | PASS |
| **Approximate Entropy Test** | P_value | 0.718234 | 0.851571 |
| | status | PASS | PASS |

TABLE VII CONT.

| Test ID | | ***u*** | ***v*** |
|---|---|---|---|
| **Cumulative Sums forward Test** | P_value | 0.331430 | 0.468936 |
| | status | PASS | PASS |
| **Cumulative Sums Reverse Test** | P_value | 0.414308 | 0.774705 |
| | status | PASS | PASS |
| **Random Excursions Test** | P_value (mean) | 0.3277 | 0.5884 |
| | status | PASS | PASS |
| **Random Excursions Variant Test** | P_value (mean) | 0.2607 | 0.5167 |
| | status | PASS | PASS |

## REFERENCES

[1] O. Boubaker, S. Jafari, "Recent Advances in Chaotic Systems and Synchronization: From Theory to Real World Applications," Academic Press, 1st ed. , Nov. 2018.

[2] M. M. Hussain, M. Siddique, et al., "Synchronization of Chaotic Systems: A Generic Nonlinear Integrated Observer-Based Approach," Complexity, Hindawi, Volume 2021, 2021.

[3] A. S. Youssef, S. Elramly, M. Ibrahim, and A. Abdel-Hafez, "Synchronization Recovery of Chaotic Signal Through Imperfect Channel Using Optimization Approach," 6th International Conference on Internet Technology and Secured Transactions, Abu Dhabi, United Arab Emirates, pp. 73-78, December 2011.

[4] A. S. Youssef, S. Elramly, M. Ibrahim, and A. Abdel-Hafez, "Denoising Algorithm for Noisy Chaotic Signal by Using Wavelet Transform: Comprehensive Study," 6th International Conference on Internet Technology and Secured Transactions, pp. 79-85, Abu Dhabi, United Arab Emirates, December 2011.

[5] S. Hashemia, M. A. Pourmina, S. Mobayen, M. R. Alagheband, "Design of a secure communication system between base transmitter station and mobile equipment based on finite-time chaos synchronization," international journal of systems science, vol. 51, no. 11, pp1969–1986, 2020.

[6] L. Moysis, C. Volos, et al., "A Novel Chaotic System with a Line Equilibrium: Analysis and Its Applications to Secure Communication and Random Bit Generation," MDPI, Telecom, 1(3), pp283–296, 2020.

[7] S. Banerjee, "Chaos Synchronization and Cryptography for Secure Communications: Applications for Encryption," IGI Global; 1st edition, 2010.

[8] L. Kocarev and S. Lian, "Chaos-based Cryptography: Theory, Algorithms and Applications," Springer; 1st ed, 2011.

[9] H. Jinfeng , J. Guo, "Breaking a chaotic secure communication scheme," Chaos an interdisciplinary journal of nonlinear science, Vol 18, Issue 1, March 2008.

[10] G. Hu, Z. Feng, and R. Meng, "Chosen Ciphertext Attack on Chaos Communication Based on Chaotic Synchronization," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 50, no. 2, pp. 275–279, Feb. 2003.

[11] C. E. Shannon, "Communication Theory of Secrecy Systems," Bell System Technical Journal, vol.28, no. 4, pp.656-715, October 1949.

[12] H. Delfs and H. Knebl, "Introduction to Cryptography: Principles and Applications," Springer, 3rd edition, 2015.

[13] K. Seyhan, S. Akleylek, "Classification of random number generator applications in IoT: A comprehensive taxonomy," Journal of Information Security and Applications, Volume 71, December 2022.

[14] J. Stone, "Bayes' Rule: A Tutorial Introduction to Bayesian Analysis," Sebtel Press; 1st edition, December 3, 2021.

[15] "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", National Institute of Standards and Technology (NIST), Special Publication 800-22, Revision 1a, April 2010, available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf

[16] L. Kocarev and S. Lian, "Chaos-based Cryptography: Theory, Algorithms and Applications," Springer; 1st Edition, 2011.

[17] H Nagashima, "Introduction to Chaos: Physics and Mathematics of Chaotic Phenomena," CRC Press; 1st edition, June 2019.

[18] F. Anstett, G. Millerioux, and G. Bloch, "Chaotic CryptoSystems: Cryptanalysis and Identifiability," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 53, no. 12, pp.2673-2680, December 2006.

[19] N. Masuda and K. Aihara, "CryptoSystems With Discretized Chaotic Maps," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 49, no. 1, pp. 28-40, January 2002.

[20] K. Li, Y. Chai Soh, and C. Zhang, "A Frequency Aliasing Approach to Chaos-Based Cryptosystems," IEEE Transactions on Circuits and Systems—I: Regular Papers, Vol. 51, No. 12, December 2004.

**A. S. Youssef** was born on December 6th, 1976 in Cairo, Egypt. He received his Bachelor of Electronics and Communication Engineering (B.Sc.) from Ain Shames University, Cairo, Egypt, in 1999. He completed his Master, and Ph.D. in Electronics and Communication Engineering, from the same university in 2006 and 2013 respectively. He has been working at the Higher Colleges of Technology HCT in UAE since 2009. His research interests lie in the areas of signal processing and chaotic signals. He has collaborated actively with researchers in several other areas including adaptive modulation and security systems.