ADBA Computer Science
Cutting-Edge Scientific Solutions

e-ISSN: 3023-8544
RESEARCH ARTICLE
Vol.2 / No.2 / 2025 / pp.50-55
https://doi.org/10.69882/adba.cs.2025074

True Random Number Generator Design with A Fractional Order Sprott B Chaotic System

Mehmet Ziya Hoşbaş [*,1], **Berkay Emin** [α,2] **and Fırat Kaçar** [β,3]

*Department of Electronics and Automation, Technical Sciences Vocational College, Hitit University, Corum, 19100, Türkiye, αOsmancık Ömer Derindere MYO, Hitit University, Corum, 19500, Türkiye, βDepartment of Electrical and Electronics Engineering, Faculty of Engineering, Istanbul University-Cerrahpasa, Istanbul, 34320, Türkiye.

ABSTRACT The growing prevalence of digital communication and interconnected devices has amplified the need for robust data security measures. True random number generators (TRNG) play a pivotal role in protecting information by generating unpredictable and irreproducible sequences required for encryption, secure authentication, and cryptographic key generation. This research presents a TRNG model based on the fractional-order Sprott B chaotic system. The chaotic properties of the system were confirmed through Lyapunov exponent calculations, bifurcation diagrams, and phase space analyses. The fractional-order dynamics enhance the complexity and unpredictability of the generated entropy source, making it suitable for secure applications. The performance of the generated random numbers was assessed using the NIST 800-22 statistical test suite, successfully passing all tests and meeting the randomness requirements. This study introduces a unique approach by leveraging the fractional-order Sprott B chaotic system for TRNG design, demonstrating its effectiveness in cryptographic systems and secure communication frameworks.

KEYWORDS
Nonlinear dynamics
Chaos
TRNG
Fractional-order chaotic systems

INTRODUCTION

True Random Number Generators (TRNGs) have become one of the foundational components of security in modern digital systems. Applications such as cryptographic key generation, authentication, digital signatures, secure communication protocols, blockchain systems, and hardware-based security modules require high-quality and unpredictable random numbers. Especially in sensitive fields such as quantum key distribution, biometric systems, and military communications, the deterministic nature of pseudo-random number generators cannot provide sufficient security, making TRNGs based on physical entropy sources the preferred choice.

For instance, in the study conducted by Park *et al.* (2020), a physically implemented TRNG design based on beta radiation was presented and optimized for low-power IoT applications. The entropy source of the TRNG relies on ionization events caused by beta particles, enabling the generation of highly secure randomness based on external physical processes. The designed TRNG was implemented at the hardware level and successfully validated through NIST 800-22 and ENT tests, demonstrating its applicability for use in IoT devices. Such studies clearly reveal that TRNGs are not only theoretically significant but also play a critical role in real-world hardware-level applications. Therefore, the development of TRNG architectures with high entropy and irreproducibility has become more important than ever for information security.

Among recent developments, FPGA-based TRNG designs have gained significant attention in recent years due to their ability to provide both high-speed performance and hardware-level flexibility. In this context, Frustaci *et al.* (2024) proposed a DSP-based true random number generator architecture optimized for FPGA implementation. The design leverages jitter from oscillator-based entropy sources and integrates a lightweight digital signal processing scheme to enhance randomness. The generated bitstreams were subjected to the NIST 800-22 statistical test suite, with results confirming that the TRNG output possesses sufficient entropy and unpredictability for cryptographic applications. This study highlights the feasibility and importance of developing efficient and secure TRNG structures directly in reconfigurable hardware environments such as FPGAs.

Similarly, Della Sala *et al.* (2022) introduced an ultra-compact TRNG architecture that is compatible with FPGA platforms and utilizes latched ring oscillators as the entropy source. The design emphasizes area-efficiency while maintaining a high level of randomness quality suitable for cryptographic uses. By exploiting the metastability behavior of digital latches in ring oscillator configurations, the proposed system ensures a non-deterministic output stream. The statistical evaluation, including NIST 800-22 tests, confirms that the TRNG meets the criteria required for secure embedded systems. This work demonstrates the potential for implementing compact and effective TRNGs within resource-constrained hardware environments.

Manuscript received: 15 January 2025,
Revised: 16 July 2025,
Accepted: 22 July 2025.

[1]mehmetziyahosbas@hitit.edu.tr(**Corresponding author**)
[2]berkayemin@hitit.edu.tr
[3]fkacar@istanbul.edu.tr

Furthermore, Garipcan and Erdem (2020) proposed a True Random Number Generator (TRNG) architecture that utilizes ring oscillators (ROs) as the physical noise source, with true randomness extracted from jitter. To enhance the statistical quality of the raw random bitstream, they introduced a novel post-processing technique based on a chaotic entropy pool, composed of discrete-time chaotic maps including quadratic, cubic, Bernoulli shift, and tent maps. Their user-controllable and dynamically adaptable post-processing structure allows the combination of multiple chaotic systems, providing both flexibility and improved entropy. The TRNG was successfully implemented on an FPGA platform, and statistical evaluations confirmed its compliance with cryptographic standards, demonstrating its effectiveness for secure hardware applications.

Among the numerous chaotic systems introduced in the literature, the Sprott B system is particularly notable due to its simple structure and rich dynamic behavior (Sprott 2003). Unlike its counterparts, the Sprott B system offers a balance between computational efficiency and chaotic complexity, making it an ideal candidate for hardware implementations of TRNGs. Despite its potential, the Sprott B system remains underexplored in the context of random number generation, particularly in fractional-order configurations.

In recent years, fractional-order chaotic systems have gained attention for their high entropy generation capabilities, making them suitable for a variety of cryptographic applications. Their inherently complex dynamic behavior and high sensitivity to initial conditions enable them to serve as effective physical entropy sources, especially in secure data transmission and image encryption. For instance, a recent study conducted a thorough numerical analysis of a fractional-order chaotic system and successfully applied its chaotic outputs in biometric data encryption (Gokyildirim *et al.* 2024). Such implementations demonstrate that chaotic systems are not only of theoretical interest but also practically viable for security mechanisms, offering alternative entropy sources for TRNG designs.

To enhance entropy diversity in chaos-based TRNG designs, exploring systems with multiple coexisting chaotic attractors offers significant advantages. Lai and Chen (2016) proposed a polynomial function-based method to extend the dynamics of the Sprott B system, enabling the generation of multiple chaotic attractors from distinct initial conditions. Their approach increases the number of index-2 saddle foci, allowing the system to exhibit two, three, or even four coexisting chaotic attractors. These attractors were validated using standard nonlinear analysis tools such as bifurcation diagrams, Lyapunov exponent spectra, and phase portraits. This method highlights the potential of structurally simple systems like Sprott B to generate rich dynamical behaviors, making them more versatile and robust candidates for secure entropy generation in hardware-based TRNGs.

(Lai *et al.* 2019), it was demonstrated that the Sprott B system can generate multiple independent chaotic and periodic attractors under different initial conditions and system parameters. Moreover, multistability was achieved in the system using a sign function, and a controller was designed to enable transitions between the chaotic attractors. This feature is particularly valuable for TRNGs designed using fractional-order chaotic systems, as it enhances the entropy generation capacity of the system and improves the quality of randomness.

Ramamoorthy *et al.* (2022) introduces a novel four-dimensional memristive extension of the Sprott B chaotic system, revealing rich dynamical behaviors including multistability, attractor coalescence, and symmetry transitions. Notably, the system is capable of transitioning between rotational symmetry and symmetry-breaking states via a tunable bias term, resulting in coexisting chaotic attractors. These phenomena, particularly partial amplitude control and offset boosting are critical for enhancing entropy generation in chaos-based TRNG designs. Such dynamic flexibility is especially relevant when employing fractional-order chaotic systems, where maximizing entropy diversity and improving randomness quality are key requirements for cryptographic robustness. The controllable multistable behavior demonstrated in this memristive system provides valuable insights for designing advanced TRNG architectures with reconfigurable entropy sources.

In this study, a novel approach for True Random Number Generator (TRNG) design is presented by integrating the fractional-order Sprott B chaotic system. The chaotic characteristics of the system are thoroughly analyzed using standard dynamical tools such as phase portraits, and its suitability for secure entropy generation has been validated (Wolf *et al.* 1985). The generated random bit sequences have been subjected to rigorous statistical evaluations, including the NIST 800-22 test suite, to confirm compliance with global randomness standards.

This research aims to fill the literature gap by demonstrating the potential of the fractional-order Sprott B system as a reliable entropy source for TRNGs. By providing both theoretical insights and practical evaluations, the study contributes to the ongoing development of secure random number generators and offers a foundation for future research in chaos-based cryptographic systems (Jun and Kocher 1999).

FRACTIONAL ORDER SPROTT B CHAOTIC SYSTEM AND CIRCUIT REALIZATION

In 1994, Sprott (1994) introduced several chaotic systems with five and six terms, which he named A to S. These systems model chaotic behavior using simple differential equations and each of them exhibits different dynamical properties. Among them, the Sprott B chaotic system is a dynamical system described by a set of three-dimensional nonlinear differential equations and is expressed as given in Equation 1. The Sprott B system is expressed by the following autonomous differential equations:

$$\begin{aligned} \dot{x} &= yz \\ \dot{y} &= x - y \\ \dot{z} &= 1 - xy \end{aligned} \tag{1}$$

Here, x, y, and z denote the state variables.

Fractional-order differential equations provide a more comprehensive mathematical framework compared to classical differential equations. This is particularly important in the analysis and control of chaotic systems, where fractional dynamics offer enhanced realism and flexibility in modeling complex behavior. In this study, the Sprott B chaotic system is formulated using fractional-order differential equations, as presented in Equation 2.

In this formulation, x, y, and z are the state variables of the system, while q_1, q_2, and q_3 denote fractional orders of differentiation. The dynamic properties of the Sprott B system are further explored by adopting a fractional-order approach. Consequently, the system is represented as an incommensurate fractional-order chaotic model, as given in Equation 2.

$$
\begin{aligned}
D^{(q_1)}x &= yz, \\
D^{(q_2)}y &= x - y, \\
D^{(q_3)}z &= 1 - xy.
\end{aligned} \tag{2}
$$

Here, x, y, and z represent the state variables, and D^q denotes the fractional-order differential operator. Parameters a and β are system-specific constants. Fractional calculus generalizes classical calculus by introducing non-integer order derivatives and integrals, denoted as D_t^q. This operator performs differentiation for $q > 0$ and integration for $q < 0$, and encompasses several definitions such as Grünwald–Letnikov, Riemann–Liouville, and Caputo. Among these, the Caputo definition is widely preferred due to its compatibility with classical initial conditions.

The Caputo–Euler method is a numerical technique for solving fractional differential equations based on the Caputo definition. It extends the classical Euler method by approximating fractional derivatives using a discretized form of the Caputo operator. This method iteratively computes the solution over a defined time span, making it particularly suitable for the analysis of systems exhibiting fractional-order dynamics. In this study, the Caputo–Euler method is employed to numerically solve the fractional-order differential equations. Its effectiveness in capturing complex behaviors such as chaos, phase-space evolution, and bifurcations makes it a powerful tool for investigating the dynamic properties of the system.

The practical implementation of chaotic systems on embedded platforms offers valuable opportunities for various scientific and engineering applications. In this study, the Sprott B chaotic system is implemented on the Nvidia Jetson AGX Orin embedded system platform. However, since the Nvidia Jetson AGX Orin platform does not have analog output, a 16-bit resolution TI DAC8552 based converter board with SPI interface is used to convert digital signals to analog signals [2]. The converter board is controlled by software written in Python programming language. Thanks to this approach, digital outputs are converted to analog signals with high accuracy, making it possible to make the Sprott B chaotic signal directly usable in the physical world. The general structure of the system for the application is given in Figure 1. The

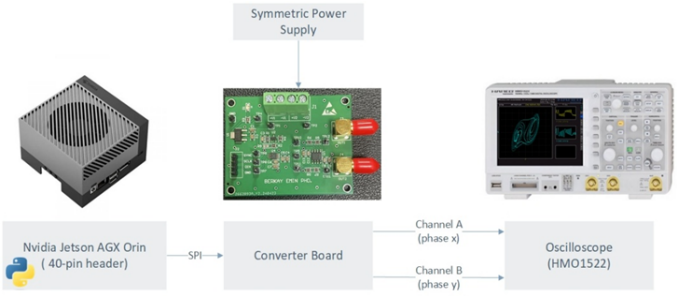

Figure 1 General structure of the implementation system.

fractional-order Sprott B chaotic System is analyzed using the Caputo definition, with a selected order of $q = 0.9$, system parameters $a = 0.8$, $\beta = 0.82$, and initial conditions $(x_0, y_0, z_0) = (1, 1, 1)$. The aim is to investigate the influence of the fractional-order parameter q on the system's dynamic and chaotic behavior. For this purpose, phase portraits and oscilloscope screenshots were generated for three different values of q: 0.9, 0.93, and 0.95. These visualizations serve to assess the sensitivity of the system to changes in its fractional dynamics.

Figure 2 illustrates the simulation results for $q = 0.9$, revealing the system's inherent chaotic nature under the specified initial conditions and parameter set. The phase-space trajectories in the x-y, y-z, and x-z planes, along with the corresponding oscilloscope views, depict well-developed chaotic attractors. Figure 3 presents the results for $q = 0.93$. Compared to the previous case, subtle changes in the structure and density of the trajectories are observed, indicating that small variations in q significantly affect the system's dynamical characteristics. Figure 4 shows the phase portraits and oscilloscope outputs for $q = 0.95$. The attractor geometry evolves further, highlighting an increase in complexity and trajectory dispersion. This demonstrates the growing sensitivity of the system's behavior as the fractional order increases.

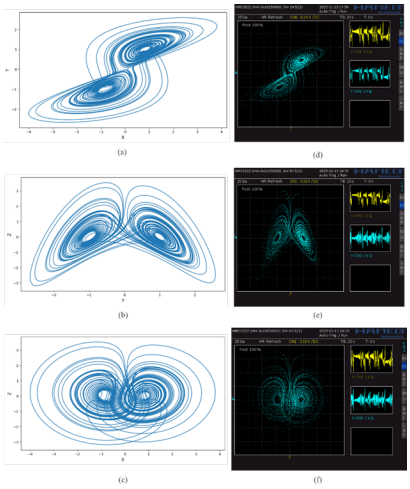

Figure 2 Phase Portraits of Fractional Order Sprott B system for $q = 0.9$; (a) phase portrait in x-y plane, (b) phase portrait in y-z plane, (c) phase portrait in x-z plane, (d) oscilloscope image of the x-y plane, (e) oscilloscope image of the y-z plane, (f) oscilloscope image of the x-z plane.

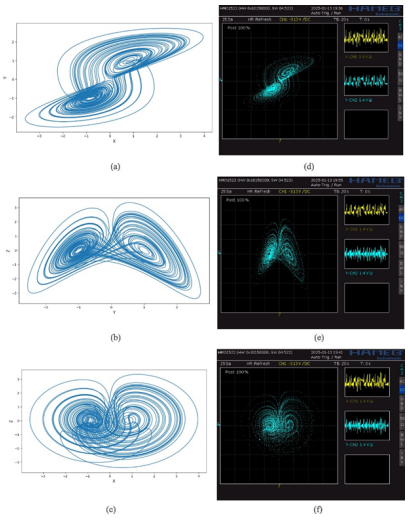

Figure 3 Phase Portraits of Fractional Order Sprott B system for $q = 0.93$; (a) phase portrait in x-y plane, (b) phase portrait in y-z plane, (c) phase portrait in x-z plane, (d) oscilloscope image of the x-y plane, (e) oscilloscope image of the y-z plane, (f) oscilloscope image of the x-z plane.

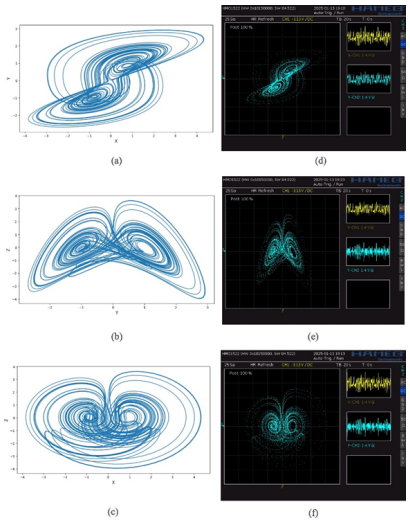

Figure 4 Phase Portraits of Fractional Order Sprott B system for $q = 0.95$; (a) phase portrait in x-y plane, (b) phase portrait in y-z plane, (c) phase portrait in x-z plane, (d) oscilloscope image of the x-y plane, (e) oscilloscope image of the y-z plane, (f) oscilloscope image of the x-z plane.

DESIGN OF A TRUE RANDOM NUMBER GENERATOR BASED ON EMBEDDED SYSTEMS

This flowchart presents the design of a True Random Number Generator (TRNG) that integrates a fractional-order Sprott B chaotic system with real-time temperature data from the Orin Nano GPU. As illustrated in Figure 5, the TRNG process follows a systematic flow to ensure high-entropy, unpredictable random bit generation.

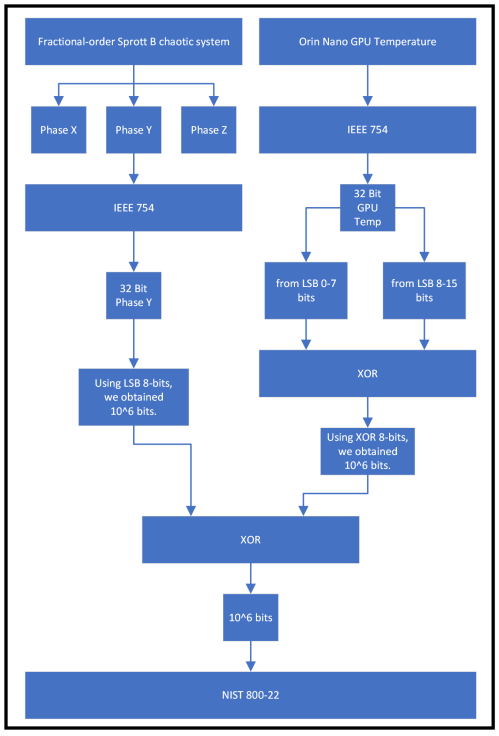

Figure 5 Flowchart of Fractional-Order Sprott B Chaotic System-based TRNG.

The design begins with the chaotic system's outputs, which consist of three phases: Phase X, Phase Y, and Phase Z. These phases are converted into 32-bit floating-point representations using the IEEE 754 standard. Specifically, the Phase Y output is chosen for further processing. The least significant 8 bits (LSB) from this 32-bit value are extracted to form a large dataset of random bits. This step is crucial since the LSBs in chaotic signals are typically the most unpredictable and contribute significantly to randomness. Simultaneously, the system records real-time temperature data from the Orin Nano GPU, which also undergoes conversion into a 32-bit floating-point format following the IEEE 754 standard. The system extracts two specific byte ranges from the 32-bit temperature value: the first 8 bits (LSB) and the second byte (bits 8 to 15). These two segments are combined using an XOR (exclusive OR) operation to form another sequence of random bits. This step leverages environmental variability, as temperature fluctuations introduce physical randomness.

The two independent sequences, one from the chaotic system and the other from the temperature sensorare then merged using a second XOR operation. This final XOR combination blends deterministic chaotic dynamics with physical randomness, ensuring a highly complex and unpredictable final sequence of 10^6 bits. To validate the quality of the generated random sequence, it is subjected to the NIST 800-22 statistical test suite, a widely recognized standard for evaluating randomness. This test suite assesses various properties such as uniform distribution, independence, and unpredictability to ensure the output meets stringent international randomness standards.

In summary, the integration of the fractional-order Sprott B chaotic system and the real-time temperature data ensures that the TRNG produces a robust and secure random bit sequence. The use of chaotic phase data and temperature readings, combined through XOR operations, enhances entropy and reduces any potential correlations, making this approach suitable for cryptographic applications. The results of the NIST 800-22 statistical tests demonstrate that the random bit sequence generated by the True Random Number Generator (TRNG) meets rigorous international randomness standards. A detailed interpretation of these results is presented in Table 1.

Table 1 NIST 800-22 Test Results for Sprott B Chaotic System-Based TRNG

Test Type	P-Value	Conclusion
Frequency Test (Monobit)	0.0672	Passed
Frequency within a Block	0.3761	Passed
Run Test	0.5410	Passed
Longest Run of Ones	0.3397	Passed
Binary Matrix Rank	0.3633	Passed
DFT (Spectral) Test	0.4408	Passed
Non-Overlapping Template	0.2993	Passed
Overlapping Template	0.0591	Passed
Maurer's Universal	0.6973	Passed
Linear Complexity	0.9899	Passed
Serial Test 1	0.3801	Passed
Serial Test 2	0.5467	Passed
Approximate Entropy	0.1549	Passed
Cumulative Sums (Forward)	0.0440	Passed
Cumulative Sums (Reverse)	0.1162	Passed
Excursions Test (-4)	0.9233	Passed
Excursions Variant (-9)	0.5929	Passed

The Frequency Test (Monobit) confirms that the number of 1s and 0s in the sequence is approximately equal, indicating a balanced distribution. Similarly, the Frequency Test within a Block verifies that the balance of 1s and 0s is maintained across different blocks of the sequence. The Run Test ensures that the lengths of consecutive sequences of identical bits (runs of 0s or 1s) match expected distributions for a random sequence. The Longest Run of Ones in a Block test further supports this by checking the longest sequence of 1s in each block, confirming that the bitstream does not exhibit unusual clustering.

The Binary Matrix Rank Test evaluates the rank of matrices formed from the bit sequence to detect any linear dependencies. The results show no significant linear patterns, reinforcing the randomness of the sequence. The Discrete Fourier Transform (Spectral) Test checks for periodic features and verifies the absence of predictable repeating patterns.

The Non-Overlapping Template Matching Test and Overlapping Template Matching Test search for predefined patterns in the sequence. The passing results indicate that the sequence does not show excessive occurrences of specific bit patterns, suggesting that the sequence is unpredictable. The Maurer's Universal Statistical Test assesses the compressibility of the sequence. The high p-value suggests that the sequence is incompressible and, therefore, random. Similarly, the Linear Complexity Test measures the complexity of the sequence by determining the shortest feedback register that could generate it. The passing result indicates that the sequence cannot be generated by a simple process.

The Serial Test checks the uniformity of overlapping bit patterns, and both sub-tests confirm that the sequence maintains a balanced distribution of these patterns. The Approximate Entropy Test further validates the sequence by ensuring that it does not contain repeating patterns beyond what would be expected in a random sequence. The Cumulative Sums (Forward and Reverse) Test examines the cumulative sum of the sequence in both forward and reverse directions, confirming that the bitstream behaves as expected for a truly random sequence.

The Random Excursions Test evaluates the number of times the cumulative sum of the sequence visits specific states within a defined range. The results show that the transitions through these states occur at frequencies consistent with random behavior. The Random Excursions Variant Test extends this analysis to a larger range of states and similarly indicates that the state transitions are consistent with randomness. In summary, the TRNG passes all tests in the NIST 800-22 suite, demonstrating that the generated sequence is uniformly distributed, free from detectable patterns, and unpredictable. These results confirm the effectiveness of the TRNG based on the fractional-order Sprott B chaotic system, making it a reliable solution for secure cryptographic applications that require high-quality random sequences.

CONCLUSION

This study presents the design and implementation of a True Random Number Generator (TRNG) based on a fractional-order Sprott B chaotic system, demonstrating its potential as a secure entropy source for cryptographic applications. By leveraging the unique properties of fractional-order dynamics, the system enhances the unpredictability and complexity of the generated random sequences. The Caputo–Euler method was employed to solve the fractional differential equations accurately, ensuring precise modeling of the chaotic behavior. The integration of environmental entropy, in the form of real-time temperature readings from the Nvidia Jetson AGX Orin platform, further strengthens the randomness of the generated bitstreams. The combination of chaotic phase data and physical randomness using XOR operations results in a highly secure and robust random bit sequence.

The performance of the proposed TRNG was rigorously validated through the NIST 800-22 statistical test suite, where the system passed all randomness tests. This confirms that the generated sequences exhibit uniform distribution, independence, and unpredictability, satisfying stringent global randomness standards. In conclusion, the fractional-order Sprott B chaotic system provides a promising basis for TRNG design by combining mathematical richness with efficient implementation. The results indicate that this method can be effectively used in secure communication and cryptographic applications. Future work may focus on optimizing the hardware implementation and exploring the use of other fractional-order chaotic systems to further enhance entropy generation.

Ethical standard

The authors have no relevant financial or non-financial interests to disclose.

Availability of data and material

Not applicable.

Conflicts of interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

LITERATURE CITED

Della Sala, R., D. Bellizia, and G. Scotti, 2022 A novel ultra-compact fpga-compatible trng architecture exploiting latched ring oscillators. IEEE Transactions on Circuits and Systems II: Express Briefs **69**: 1672–1676.

Frustaci, F., F. Spagnolo, P. Corsonello, and S. Perri, 2024 A high-speed and low-power dsp-based trng for fpga implementations. IEEE Transactions on Circuits and Systems II: Express Briefs **71**: 4964–4968.

Garipcan, A. M. and E. Erdem, 2020 A trng using chaotic entropy pool as a post-processing technique: analysis, design and fpga implementation. Analog Integrated Circuits and Signal Processing **103**: 391–410.

Gokyildirim, A., S. Çiçek, H. Calgan, and A. Akgul, 2024 Fractional-order sprott k chaotic system and its application to biometric iris image encryption. Computers in Biology and Medicine **179**: 108864.

Jun, B. and P. Kocher, 1999 The intel random number generator. Technical report, Cryptography Research, Inc.

Lai, Q. and S. Chen, 2016 Generating multiple chaotic attractors from sprott b system. International Journal of Bifurcation and Chaos **26**: 1650177.

Lai, Q., G. Xu, and H. Pei, 2019 Analysis and control of multiple attractors in sprott b system. Chaos, Solitons & Fractals **123**: 192–200.

Park, J.-M., J.-W. Lee, T.-W. Oh, Y.-H. Kim, and S.-C. Hong, 2020 A lightweight true random number generator using beta radiation for iot applications. ETRI Journal **42**: 899–909.

Ramamoorthy, R., K. Rajagopal, G. D. Leutcho, O. Krejcar, H. Namazi, *et al.*, 2022 Multistable dynamics and control of a new 4d memristive chaotic sprott b system. Chaos, Solitons & Fractals **156**: 111834.

Sprott, J. C., 1994 Some simple chaotic flows. Physical Review E **50**: 647–650.

Sprott, J. C., 2003 A simple chaotic circuit. IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing **45**: 716–717.

Wolf, A., J. B. Swift, H. L. Swinney, and J. A. Vastano, 1985 Determining lyapunov exponents from a time series. Physica D: Nonlinear Phenomena **16**: 285–317.

How to cite this article: Hoşbaş, M. Z., Emin, B., and Kaçar, F. True Random Number Generator Design with A Fractional Order Sprott B Chaotic System. *ADBA Computer Science*, 2(2), 50-55, 2025.