

A Dormand-Prince Based Hybrid Chaotic True Random Number Generator on FPGA

İ. KOYUNCU, H. İ. ŞEKER, M. ALÇIN and M. TUNA

Abstract— This study presents a Dormand-Prince-based hybrid chaotic True Random Number Generator Design (TRNG) that can be used for secure communication and cryptographic applications on Field Programmable Gate Array (FPGA). In this design, a chaotic oscillator unit has been implemented with an FPGA-based Sprott-Jafari chaotic oscillator model suitable with IQ-Math fixed point number and IEEE 754-1985 floating point number standards. Random numbers have been produced with the quantization of the results generated by the chaotic oscillator. XOR has been performed with FPGA-based ring oscillator structure on the post-processing unit so as to enhance the randomness. The differential equation of the chaotic system used in the TRNG design was modelled using Dormand-Prince numerical algorithm method. The design on FPGA has been realized in two separate number formats including 32-bit (16I-16Q) IQ-Math fixed point number standard and 32-bit IEEE 754-1985 floating point number standard. The realized design has been coded in VHDL, a hardware description language, and the Xilinx ISE 14.7 program has been used for the system design. The TRNG design has been synthesized and tested for the Virtex-6 (XC6VLX240T-1FF1156) FPGA chip. The maximum operating frequencies of the TRNG in 32-bit IQ-Math fixed point number standard and 32-bit IEEE 754-1985 floating point number standard reach 344.585 MHz and 316 MHz, respectively. The throughputs of the TRNG in 32-bit IQ-Math fixed point number standard and 32-bit IEEE 754-1985 floating point number standard have been obtained as 344 Mbit/s and 316 Mbit/s, respectively. 1 Mbit sequence has been generated by using TRNG system. Randomness analysis of the generated numbers has been

performed in accordance with the NIST 800-22 tests and the generated numbers have successfully passed all of the tests.

Index Terms— Dormand-Prince Algorithm, IQ-Math number standard, Chaotic System, FPGA.

I. INTRODUCTION


Chaotic systems are defined as complex, nonlinear dynamical systems that are highly sensitive to initial conditions with irregular behavior [1].

Numerous national and international studies have been conducted on chaos and chaotic systems in recent years. Control [2], biomedical [3, 4], secure communication [5, 6], image processing [7, 8], fuzzy logic [9], artificial neural networks [10, 11], random number generators [12, 13], industrial control [14, 15], secure communication [16] and cryptography [17] can be given as examples of these studies.


Cryptography is defined as a series of techniques that need to be performed for data encryption and decryption due to its nature. The practice and study fields of chaotic signals include secure communication, cryptography and Random Number Generators (RNGs). Random numbers generated by RNG are used to form the initial vector, private and secret keys in cryptography. These keys can be produced as embedded off- or on-system. Off-system embedment weakens the security. Therefore, this is performed through digital circuits-based platforms such as hardware-based Digital Signal Processors (DSP) [18, 19], Application Specific Integrated Circuits (ASIC) [20, 21], and Field Programmable Gate Array (FPGA) [22, 23] to remove this disadvantage. True Random Number Generators (TRNGs) are essential for cryptology and secure communication practices. It is important for these random numbers used to display powerful statistical features, unpredictability and have regular distribution in terms of cryptography. The TRNGs have three main stages [24]. First stage includes the entropy resource which generates random numbers. Second stage includes quantification process which is described as generation of random number bits by using the randomness of entropy resource. Third stage includes post-processing blocks to strengthen statistical features [25].

Studies on FPGA-based chaotic TRNG studies are increasing in the literature [12, 26-37]. Koyuncu et al. [12] designed chaos-based TRNG design on Xilinx Virtex-6 FPGA using the Sundarapandian-Pehlivan chaotic system using the design based on RK4 numerical algorithm. In another study, Fischer et al. [27] realized the PLL based oscillator with


ISMAIL KOYUNCU is with Afyon Kocatepe University, Department of Electrical-Electronics Engineering, Afyon, 03100, TURKEY, (e-mail: ismailkoyuncu@aku.edu.tr).

 <https://orcid.org/0000-0003-4725-4879>


H. İBRAHİM ŞEKER is with Sakarya University of Applied Sciences, Department of Electrical-Electronics Engineering, Graduate Education Institute, Sakarya 54187, TURKEY, (e-mail: hseker5@gmail.com).

 <https://orcid.org/0000-0002-5343-2419>

MURAT ALÇIN is with Afyon Kocatepe University, Department of Mechatronics Engineering, Afyon, 03100, TURKEY, (e-mail: muratalcin@aku.edu.tr).

 <https://orcid.org/0000-0002-2874-7048>

MURAT TUNA is with Kırklareli University, Vocational School of Technical Sciences, Kırklareli 39060, TURKEY, (e-mail: murat.tuna@klu.edu.tr).

 <https://orcid.org/0000-0003-3511-1336>

Manuscript received April 25, 2020; accepted September 10, 2020.

DOI: [10.17694/bajece.722911](https://doi.org/10.17694/bajece.722911)

FPGA chips. Avaroğlu et al. [29] implemented chaos-based post-processing on the ring oscillator based TRNG system on Altera FPGA board. Although the operating frequency of the design they realized was high as 450 MHz, the throughput decreased after the post-processing unit as 25 Mbit/s. Alçın et al. [31] designed ANN-chaos based TRNG on Xilinx FPGA. The operating frequency of the designed system is 231.616 MHz and the bit generation rate is 115.794 Mbit/s. Tuna et al. [32] implemented a dual entropy core TRNG design using hybrid ANN-based chaotic and ring oscillator structures on FPGA. Garipcan et al. [34] designed a hybrid TRNG on FPGA. In the hybrid system they designed, they used the ring

system and the discrete-time chaotic maps system as the source of entropy. The discrete-time chaotic maps system operates as the slow oscillator and the ring system operates as the fast oscillator. The system has an operating frequency of 200 MHz and bit production rate of 15.4 Mbit/s. In Table 1, detailed information about TRNG designs and technical features designed on FPGA is given. As can be seen in the table, some studies have high operating frequencies, but bit generation rates decrease due to the algorithm used in the post-processing algorithm. The FPGA-based TRNG structure proposed in this study has the advantages of both high operating frequency and no reduction in throughput.

TABLE I
THE TECHNICAL PROPERTIES OF THE DESIGNED FPGA-BASED TRNGS IN RECENT YEARS

References	FPGA chip used	Designed Entropy type	Opr. Freq. (MHz)	Data rate (Mbit/s)
[12] Koyuncu et al.	Virtex-6	Chaotic system	293	58.76
[26] Wiczorek et al.	Spartan-3	Dual-metastability F/F	50	5
[27] Fischer et al.	Altera Stratix	PLL oscillator	250	1.0
[28] Lozach et al.	Virtex-2	Multi-ring oscillator	40	2.5
[29] Avaroğlu et al.	Altera	Ring oscillator+chaos-based post-processing	450	25
[30] Tuncer et al.	Cyclone IV	Ring oscillator	200	4.77
[31] Alçın et al.	Virtex-6	3D ANN-based	231.61	115.7
[32] Tuna et al.	Virtex-6	4D Hyperchaos+Ring	167.47	167.47
[33] Kaya et al.	Quartus-II	Chua+RO-based PUF	-----	-----
[34] Garipcan et al.	Altera	Chaotic map+Ring	200	15.4
[35] Tuncer	Altera	Chaotic map+Ring	50	2.17
[36] Prakash et al.	Virtex-6	4-D hyperchaotic system	370.894	185.447
[37] Koyuncu et al.	Virtex-6	3-D chaotic system+Ring	464	464
This study	Virtex-6	SJ Chaotic+Ring	316.756	316.756

This study presents a TRNG design that uses 32-bit IEEE 754-1985 floating point number standard and IQ-Math fixed point number standard for cryptography and secure communication. The study has compared the chip statistics and operating frequencies of two different TRNG designs. The second section gives information about chaos and introduces the Sprott-Jafari chaotic system (SJCS). The SJCS was mathematically modeled and its time series and phase portraits were presented. The SJCS-based TRNG designs suitable with two separate number formats including 32-bit IQ-Math fixed point number standard and 32-bit IEEE 754-1985 floating point number standard were implemented on FPGA by using this chaotic system. NIST tests were performed for the random numbers obtained from the TGNR models of which designs were realized, and the results were presented in comparison.

II. DORMAND-PRINCE ALGORITHM AND SPROTT-JAFARI CHAOTIC SYSTEM

Chaotic systems are defined as complex, nonlinear dynamical systems that are highly sensible to their initial conditions with random irregular behaviors. Chaotic systems are defined with differential equations. The Eq. 1 presents a differential equation belonging to the SJCS. x , y and z in this equation are the chaotic state variables. The Eq. 2 presents the system parameters and initial conditions. Minor change on the system parameters and initial conditions may affect the chaotic behavior of the system at a considerable extent. Initial

condition values of the chaotic system were determined to be $x(0)=0$, $y(0)=3.9$ and $z(0)=0.7$, and the system parameters were determined to be $a=8.888$ and $b=4$ [38].

$$\begin{aligned} dx/dt &= y \\ dy/dt &= -x + yz \end{aligned} \quad (1)$$

$$dz/dt = z + ax^2 - y^2 - b$$

$$\begin{aligned} a &= 8.888, b = 4 \\ x_0 &= 0, y_0 = 3.9, z_0 = 0.7 \end{aligned} \quad (2)$$

Chaotic systems are defined by differential equations and according to the relevant literature; the solutions of these differential equations can be modelled using various numerical algorithms such as Euler [39], Heun [40], RK4 [41] and RK5-Butcher [42]. In the presented study, the designed chaotic oscillator structure was modeled using the Dormand Prince (DP) numerical algorithm which generates more sensitive solutions than other methods.

Chaotic systems are sensitively dependent on the initial conditions and the system parameters. For this reason, changes in the system parameters and the initial conditions disrupt the chaotic behavior of the system. In other words, the system parameters and initial conditions in Eq. 2 in the SJCS system

are also specific to this chaotic system. When the parameters in Eq. 2 are changed, the chaotic dynamic behavior of the system changes. The system may not demonstrate a chaotic dynamic behavior when the specified parameter and initial conditions are out of range.

The Eq. 3 presents equation of the DP numeric algorithm [43]. Expressions that contain the derivative of a function as unknown are called differential equations. If an $f(x, y)$ function given as $f: \mathfrak{R} \rightarrow \mathfrak{R}$ and $x, y \in \mathfrak{R}$ and its derivative is defined and it is known, the values of function and its derivatives which are defined at y_i and the function values at a distance of $h = y_{i+1} - y_i$ from y_i for $i=1$ can be calculated using the Taylor series expansion. When DP numerical algorithm is examined, y_i is the initial values of the algorithm, y_{i+1} is the first result value obtained by using the initial values, and h is the number of steps.

$$\begin{aligned}
 y_{i+1} &= y_i + h \left(\frac{35}{384} k_1 + \frac{500}{1113} k_3 + \frac{125}{192} k_4 - \frac{2187}{6784} k_5 + \frac{11}{84} k_6 \right) \\
 k_1 &= F(x_i, y_i) \\
 k_2 &= F(x_i + \frac{h}{5}, y_i + \frac{h}{5} k_1) \\
 k_3 &= F(x_i + \frac{3}{10} h, y_i + \frac{3}{40} k_1 + \frac{9}{40} k_2) * h \\
 k_4 &= F(x_i + \frac{4}{5} h, y_i + \frac{44}{45} k_1 - \frac{56}{15} k_2 + \frac{32}{9} k_3) * h \\
 k_5 &= F(x_i + \frac{8}{9} * h, y_i + \frac{19372}{6561} k_1 - \frac{25360}{2187} k_2 + \frac{64448}{6561} k_3 - \frac{212}{729} k_4) * h \\
 k_6 &= F(x_i + 1 * h, y_i + \frac{9017}{3168} k_1 - \frac{355}{33} k_2 + \frac{46732}{5247} k_3 + \frac{49}{176} k_4 - \frac{5103}{18656} k_5) * h \\
 k_7 &= F(x_i + 1 * h, y_i + \frac{35}{384} k_1 + 0 * k_2 + \frac{500}{1113} k_3 + \frac{125}{192} k_4 - \frac{2187}{6784} k_5 + \frac{11}{84} k_6) * h
 \end{aligned} \quad (3)$$

The literature has various analysis methods for the chaos analysis of dynamic systems. For example, Lyapunov exponents [45], frequency spectrum [46], time-series analysis [47], bifurcation diagram [48], phase portraits and power spectrum [49]. This study used phase portrait and time-series analyses for chaos analysis of the SJCS [50]. Fig. 1 presents the SJCS's phase portraits which were obtained using the Matlab-based DP numerical algorithm. The phase portrait of a chaotic system begins to fill its orbit over time in the phase space region, it never closes over and repeats continuously. If

the system fills the phase space in this way, it indicates that it has chaotic signs. Chaotic phase portraits of 3D chaotic system can be examined as x-y, x-z, y-z and x-y-z. Phase portraits of the SJCS chaotic system obtained using the Matlab program are given in Fig. 1. As can be seen from the figure, the phase portraits of the presented system show a chaotic behavior.

Due to the sensitive dependence of chaotic systems on initial conditions, different initial values given to the system can produce different chaotic signals in a certain time. Time series analysis of the system is performed to observe the chaotic signals produced with different initial values. In Fig. 2, x, y, z and x-y-z time series of the Matlab based SJCS chaotic system are given.

III. RING OSCILLATORS

Displayed Ring oscillators compose of an odd number of NOT gates which are connected consecutively. The output of each NOT gate is connected to the next gate and the output of last NOT gate is connected to the input of the first gate. Ring oscillators generate a square wave at a frequency depending on the delays of the ring to which it is connected. The frequency of the generated square wave changes based on the static and dynamic factors of the NOT gate constituting the ring. In other words, the operating frequencies of the signals generated by two ring oscillators arranged equivalently will not be same. This can be used to generate random bits. Fig. 3 represents the structure of the ring oscillator [37].

In this study, a ring oscillator that can operate in synchronization with the chaotic oscillator was designed. The random numbers, which were generated by the ring oscillator, designed on FPGA, and the chaotic system-based random numbers were combined in the post-processing stage. The aim of this process was to form TRNG structures that have more powerful statistical features as a result of the combination of two structures.

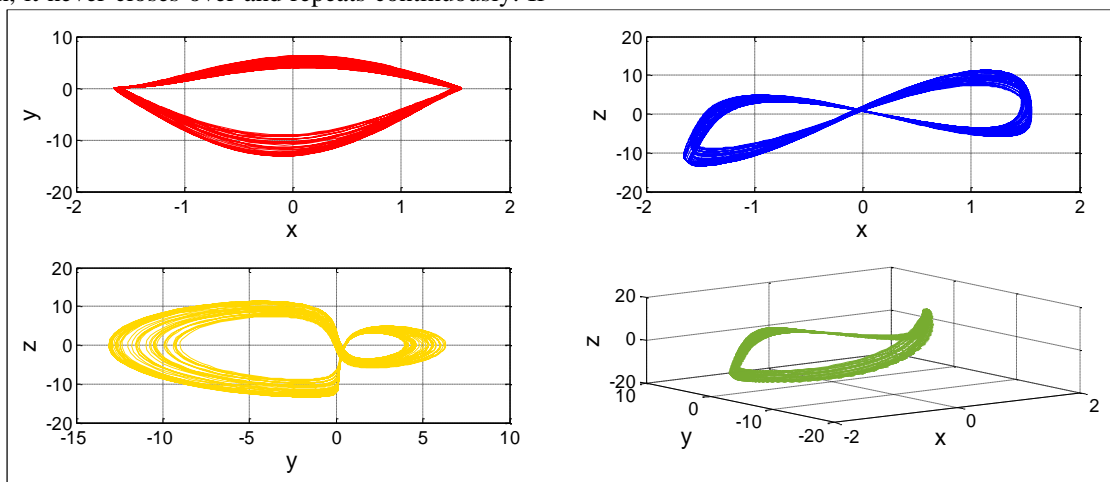


Fig. 1. The SJCS's DP numeric algorithm-based phase portraits on Matlab.

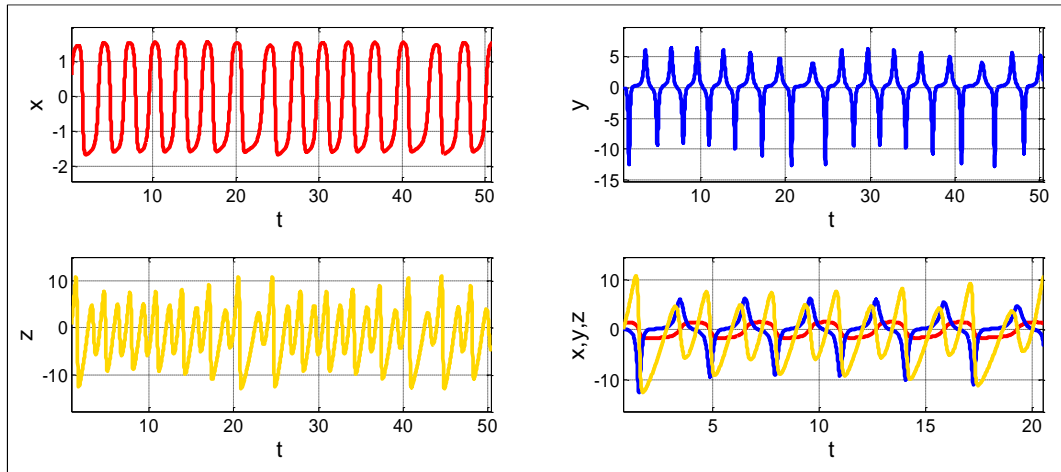


Fig. 2. The SJCS's DP numeric algorithm-based time-series analysis on Matlab.

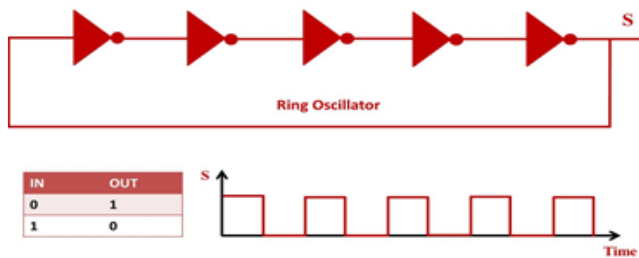


Fig. 3. Structure of the ring oscillator.

IV. CHAOTIC BASED TRNG DESIGNS ON FPGA AND RESULTS OF STATISTICAL TESTS

The SJCS-based TRNG was implemented to be operating on FPGA suitable with 32-bit (16I-16Q) IQ-Math fixed point number standard and 32-bit IEEE 754-1985 floating point number standard by using the DP numeric algorithm. The realized designs of TRNGs were coded using VHDL language. Main units used on the TRNG system design such as multiplier, adder, divider and subtractor were formed using the IP-Core Generator developed by Xilinx. The block diagrams of the recommended FPGA-based TRNGs that uses 32-bit IQ-Math fixed point number standard and SJCS-based 32-bit IEEE 754-1985 floating point number standard were similar. Fig. 4 presents the block diagram of the TRNG structure. 1-bit START signal on the input of the TRNG unit generates the signal to start the system, and 1-bit CLK clock pulse signal synchronizes the sub-units in the TRNG unit. 1-bit TRNG_SH signal on the output of the TRNG unit displays the value of 0 until the system result is ready and when the system result is ready, it displays the value of 1. 1-bit TRNG_RESULT indicates the signal that conveys the true random number values.

The proposed structure consists of four main parts including the SJCS oscillator unit, the random shredder function unit, the ring oscillator unit and the XOR unit. The SJCS oscillator unit generates the chaotic signals that TRNG needs. The

random shredder function unit uses the fractional part values of x, y and z chaotic signals and makes random selection, and then sends the result to the XOR unit. A ring oscillator that operates in synchronization with the chaotic system is available. The ring oscillator generates 1-bit values and sends them to the XOR unit. At the last phase, XOR operation is applied to the chaotic signal-based random number and the numbers that are generated by the ring oscillator. KS_SH signal gets the value of '1' when the result of the chaotic signals is present and activates the random shredder function unit to which it is attached. On the other hand, RS_SH signal generates the value of '1' when random numbers are present and activates the XOR unit, thus making it operate.

The recommended SJCS-based TRNG design at two separate number formats, which were realized on FPGA, is synthesized on the Xilinx Virtex-6 (XC6VLX240T-1FF1156) chip. The design was coded in VHDL language in accordance with 32-bit (16I-16Q) IQ-Math fixed point number standard and 32-bit IEEE 754-1985 floating point number standard. Fig. 5 presents Xilinx ISE 14.7 simulation results of 32-bit IEEE 754-1985 floating point number-based TRNG design which were realized on FPGA. Fig. 6 presents Xilinx ISE 14.7 simulation results of 32-bit IQ-Math fixed point number-based TRNG which were realized on FPGA.

SJCS-based TRNG designs, which were made using DP numeric algorithm to operate on FPGA chips, were synthesized on the Xilinx Virtex-6 (XC6VLX240T-1FF1156) chip. The synthesizing process was performed using the Xilinx ISE Design Tools. Table 2 presents the chip statistics and operating frequencies of TRNG designs which were obtained following the Place & Route process. The maximum operating frequency of 32-bit IQ-Math fixed point number-based TRNG was 344.585 MHz and the throughput was 344.5 Mbit/s. The maximum operating frequency of the TRNG at 32-bit IEEE 754-1985 floating point number standard was 316.706 MHz and the throughput was 316.7 Mbit/s. The comparison of the chip statistics on Table 2 indicated that the TRNG that uses 32-bit floating point number standard used more chip

resources and had lower operating frequency than the TRNG that uses 32-bit fixed point number standard. However, floating point number standard can generate more sensible solutions than fixed point number standard. TRNG that uses 32-bit fixed point number standard used less chip resources and had higher operating frequency. The state of randomness and statistical features of the random number generators which will be used in cryptography and secure communication should be tested. One million data set, which generated by TRNG units, were recorded in a file. NIST 800-22 test was performed on these data and the results are given on Table 3.

NIST Test Suite is an internationally validated statistical test developed to determine whether the generated bit strings are random. In order for the bit stream to be accepted as random, it must pass all tests successfully. P-value, which is

one of the most important parameters in these tests, is accepted as a measure of the randomness of the random sequences that are tested. For a random bit sequence, the P-value is close to 1, otherwise, the P-value is close to 0. In literature, P-value is generally accepted as 0.01. In other words, if the P-value is greater than 0.01, the bit sequences produced by the designed TRNG / PRNG are considered successful from the relevant test. As can be observed from Table 3, the bit sequences produced by the TRNG design presented in the study successfully passed the NIST Test Suite.

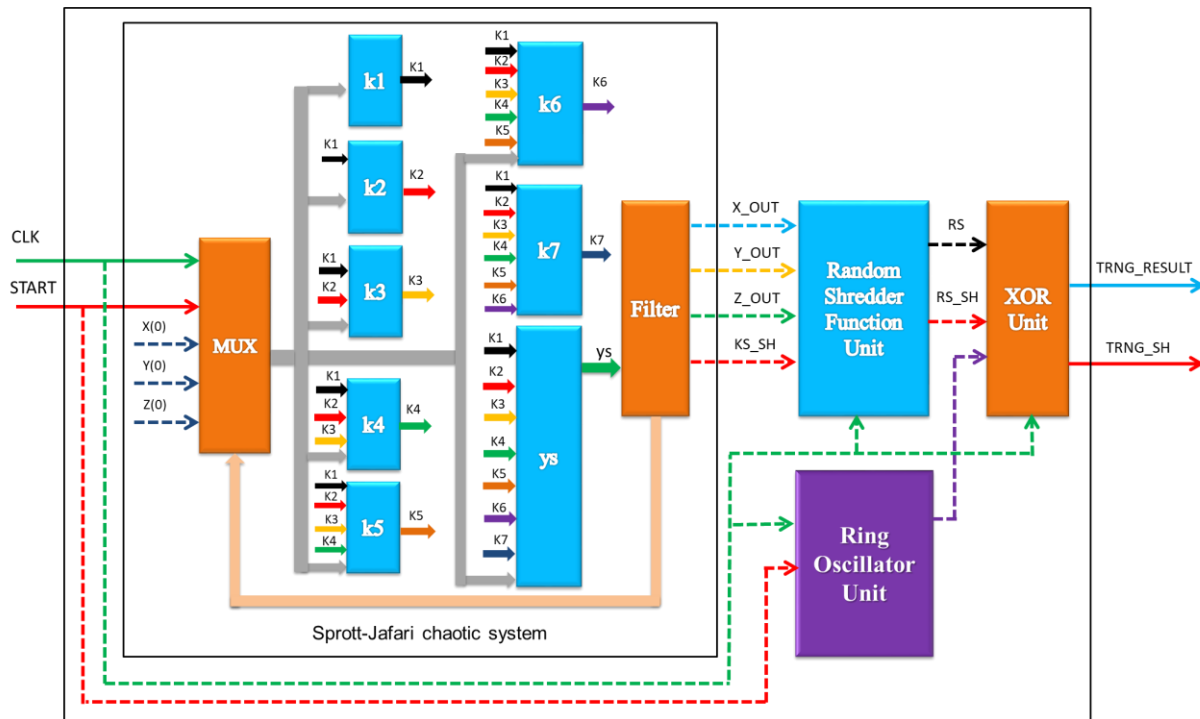


Fig. 4. Block diagram of the recommended SJCS-Ring-based TRNG design.

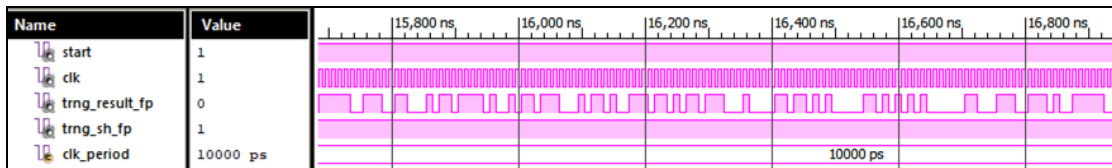


Fig. 5. Simulation results of 32-bit IEEE 754-1985 floating point number-based TRNG.

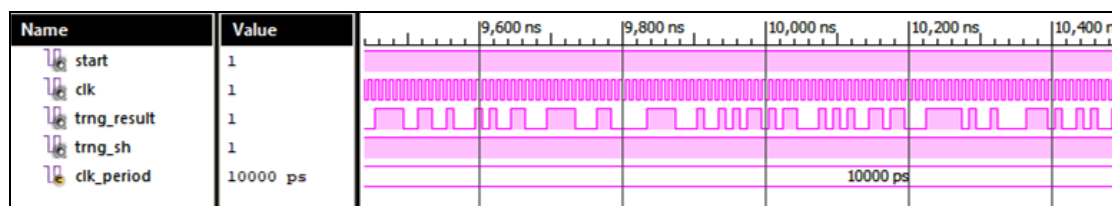


Fig. 6. Simulation results of 32-bit IQ-Math fixed point number-based TRNG.

TABLE II
CHIP STATISTICS OF DORMAND-PRINCE-BASED HYBRID CHAOTIC TRNG USING 32-BIT IQ-MATH FIXED POINT AND 32-BIT IEEE 754-1985 FLOATING POINT.

Device Utilization	32-bit IQ-Math fixed point based TRNG		32-bit IEEE 754-1985 floating Point based TRNG	
	Used/Available	Utilization	Used/Available	Utilization
	Number of Slice Registers	18507/301440	6 %	149071/301440
Number of Slice LUTs	14916/150720	9 %	147696/150720	97 %
Number of IOBs	4/600	1 %	4/600	1 %
Number of BUFG/BUFGCTRLs	1/32	3 %	1/32	3 %
Number of DSP48E1s	712/768	92 %	206/768	26 %
Max. Operating Frequency (MHz)	344.585		316.706	

TABLE III
NIST 800-22 STATISTICAL TEST RESULTS OF THE RECOMMENDED SJCS-BASED TRNG ON FPGA

NIST 800-22 Statistical Tests	Fixed Point Number Based TRNG		Floating Point Number Based TRNG	
	P value	Result	P value	Result
	Frequency test	0.44367	Successful	0.96490
Block frequency test	0.62741	Successful	0.84124	Successful
Runs test	0.46871	Successful	0.37994	Successful
Longest-run test	0.72805	Successful	0.46004	Successful
Binary matrix rank test	0.61168	Successful	0.82406	Successful
Discrete fourier transform test	0.06511	Successful	0.25516	Successful
Non-overlapping templates test	0.03843	Successful	0.03077	Successful
Overlapping templates test	0.95936	Successful	0.75952	Successful
Maurer's universal statistical test	0.06970	Successful	0.36890	Successful
Linear complexity test	0.63663	Successful	0.18509	Successful
Serial test 1	0.43141	Successful	0.65730	Successful
Serial test 2	0.69996	Successful	0.28525	Successful
Approximate entropy test	0.53332	Successful	0.54052	Successful
Cumulative-sums test	0.13721	Successful	0.97330	Successful

V. CONCLUSIONS

In this study, a chaotic oscillator unit has been performed by modeling SJCS on FPGA in 32-bit IQ-Math fixed point number standard and 32-bit IEEE 754-1985 floating point number standard. Signals generated from the unit were sent to random shredder function unit and random numbers were obtained from the signals generated by the chaotic system. To strengthen the statistical features of these numbers and to increase the rate of randomness, they were sent to post-processing unit and XOR logic operation was performed following with the generation of true random numbers. The system was coded in VHDL using the Xilinx ISE 14.7 program. The design was then synthesized and tested for the

Virtex-6 (XC6VLX240T-1FF1156) FPGA chip. The maximum operating frequencies of the TRNG in 32-bit IQ-Math fixed point number standard and 32-bit IEEE 754-1985 floating point number standard were 344.585 MHz and 316 MHz, respectively. The throughputs of the TRNG in 32-bit IQ-Math fixed point number standard and 32-bit IEEE 754-1985 floating point number standard were 344 Mbit/s and 316 Mbit/s, respectively. The sequence of 1 Mbit, which was obtained by realizing SJCS-based TRNG system both in 32-bit fixed point number standard and 32-bit floating point number standard on FPGA, was recorded in a file and was subjected to NIST 800-22 test, an international randomness test. The test results were successful. This study found that SJCS-based TRNG system, which was realized on FPGA, can be used in cryptography and secure communication.

ACKNOWLEDGMENTS

This research has been supported by grant number 18.FEN.BİL.50 from Afyon Kocatepe University Scientific Research Projects Coordination Unit.

REFERENCES

- [1] T. Bonny, and Q. Nasir, "Clock Glitch Fault Injection Attack on an FPGA-Based Non-Autonomous Chaotic Oscillator," *Nonlinear Dynamics*, vol. 96, no. 3, pp. 2087–2101, 2019.
- [2] J. S. Vaidyanathan, "Chaos in neurons and adaptive control of Birkhoff-Shaw strange chaotic attractor," *International Journal of PharmTech Research*, vol. 8, no. 5, pp. 956-963, 2015.
- [3] A. Xiong, X. Zhao, J. Han and G. Liu, "Application of the chaos theory in the analysis of EMG on patients with facial paralysis," *Robot Intelligence Techlogy and Applications*, vol. 2, no. 274, pp. 805-819, 2014.
- [4] H. Zhengxing, D. Wei, D. Huilong and L. Haomin, "Similarity measure between patient traces for clinical pathway analysis: problem, method, and applications," *IEEE Journal of Biomedical and Health Informatics*, vol. 18, no. 1, pp. 4–14, 2014.
- [5] K. Zexin, S. Jiang, M. Lin, Q. Yanhui and J. Shuisheng, "Multimode synchronization of chaotic semiconductor ring laser and its potential in chaos communication," *IEEE Journal Quantum Electron*, vol. 50, no. 3, pp. 148-157, 2014.
- [6] S. Çiçek, A. Ferikoğlu, and I. Pehlivan, "A new 3D chaotic system: dynamical analysis, electronic circuit design, active control synchronization and chaotic masking communication application," *Optik-International Journal for Light and Electron Optic*, vol. 127, no. 8, pp. 4024-4030, 2016.
- [7] E. Tlelo-Cuautle, V. H. Carbajal-Gomez, P. J. Obeso-Rodelo, J. J. Rangel-Magdaleno and J. C. Nuñez-Perez, "FPGA realization of a chaotic communication system applied to image processing," *Nonlinear Dynamics*, vol. 82, no. 4, pp. 1879-1892, 2015.
- [8] J. S. Khan and J. Ahmad, "Chaos based efficient selective image encryption," *Multidimensional Systems and Signal Processing*, vol. 30, no. 2, pp. 943-961, 2019.
- [9] X. Wang, J. H. Park, K. She, S. Zhong and L. Shi, "Stabilization of Chaotic Systems With T-S Fuzzy Model and Nonuniform Sampling: A Switched Fuzzy Control Approach," *IEEE Transactions on Fuzzy Systems*, vol. 27, no. 6, pp. 1263-1271, 2018.
- [10] M. Alçın, M. Tuna and İ. Koyuncu, "IQ-Math Based Designing of Fourth Order Runge-Kutta Algorithm on FPGA and Performance Analysis According to ANN Approximation," *Research International Journal of Advanced in Science Engineering and Technology*, vol. 5, no. 8, pp. 6523-6530, 2018.
- [11] İ. Koyuncu, İ. Şahin, C. Gloster and N. K. Sartekin, "A neuron library for rapid realization of artificial neural networks on FPGA: A case study of Rössler chaotic system," *Journal of Circuits, Systems and Computers*, vol. 26 no. 1, pp. 1750015, 2017.
- [12] İ. Koyuncu and A. T. Özcerit, "The design and realization of a new high speed FPGA-based chaotic true random number generator," *Computers & Electrical Engineering*, vol. 5, no. 8, pp. 203-214, 2017.
- [13] S. Kaçar, "Analog circuit and microcontroller based RNG application of a new easy realizable 4D chaotic system," *Optik*, vol. 127, no. 20, pp. 9551-9561, 2016.
- [14] L. dos Santos Coelho, "Tuning of PID controller for an automatic regulator voltage system using chaotic optimization approach," *Chaos, Solitons & Fractals*, vol. 39, no. 4, pp. 1504-1514, 2009.
- [15] J. Lu, X. Yu and G. Chen, "Generating chaotic attractors with multiple merged basins of attraction: A switching piecewise-linear control approach," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 50, no. 2, pp. 198-207, 2003.
- [16] Ü. Çavuşoğlu, A. Akgül, S. Kaçar, İ. Pehlivan and A. Zengin, "A chaos-based encryption algorithm over TCP data packet for secure communication," *Security and Communication Networks*, vol. 9, no.11, pp. 1285-1296, 2016.
- [17] S. Akkaya, İ. Pehlivan, A. Akgül and M. Varan, "Yeni bir kaos tabanlı rastgele sayı üretici kullanan banka şifrematik cihazı tasarımı ve uygulaması," *Journal of the Faculty of Engineering & Architecture of Gazi University*, vol. 33, no. 3, pp. 1171-1182, 2018.
- [18] R. Kharel, K. Busawon, W. Aggoune and Z. Ghassemlooy, "Implementation of a secure digital chaotic communication scheme on a DSP board," *In 2010 7th International Symposium on Communication Systems, Networks & Digital Signal Processing*, 2010: pp. 212-216.
- [19] T. Shi, G. Rui, Y. Zhang and S. Zhang, "Design Method for Duffing System Based on DSP Builder," *In 2012 International Conference on Systems and Informatics (ICSAI)*, 2012: pp. 121-124.
- [20] M. Delgado-Restituto, A. J. Acosta and A. Rodríguez-Vázquez, "A mixed-signal integrated circuit for FM-DCSK modulation," *IEEE Journal of solid-state circuits*, vol. 40, no. 7, pp. 1460-1471, 2005.
- [21] Ü. Güler and S. Ergün, "A high speed, fully digital IC random number generator," *AEU-International Journal of Electronics and Communications*, vol. 66, no. 2, pp. 143-149, 2012.
- [22] T. Bonny, R. Al Debsi, S. Majzoub, and A. S. Elwakil, "Hardware Optimized FPGA Implementations of High-Speed True Random Bit Generators Based on Switching-Type Chaotic Oscillators," *Circuits, Systems, and Signal Processing*, vol. 38, no. 3, pp. 1342–1359, 2019.
- [23] T. Bonny, and A. S. Elwakil, "FPGA Realizations of High-Speed Switching-Type Chaotic Oscillators Using Compact VHDL Codes," *Nonlinear Dynamics*, vol. 93, no. 2, pp. 819–833, 2018.
- [24] E. Avaroğlu, and T. Tuncer, "Novel S-Box-Based Postprocessing Method for True Random Number Generation", *Turkish Journal of Electrical Engineering & Computer Sciences*, vol. 28, pp. 288–301, 2020.
- [25] M. Tuna and C. B. Fidan. "A Study on the importance of chaotic oscillators based on FPGA for true random number generating (TRNG) and chaotic systems," *Journal of the Faculty of Engineering and Architecture of Gazi University*, vol. 33, no. 2, pp. 469-486, 2018.
- [26] P. Z. Wiczorek and K. Golofit, "Dual-Metastability Time-Competitive True Random Number Generator," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 61, no. 1, pp. 134–145, 2014.
- [27] V. Fischer, M. Drutarovsk, M. Simka, and N. Bochard, "High Performance True Random Number Generator in Altera Stratix FPLDs," *Field Programmable Logic and Application*, vol. 3203, pp. 555–564, 2004.
- [28] F. Lozach, M. Ben-Romdhane, T. Graba, and J.-L. Danger, "FPGA Design of an Open-Loop True Random Number Generator," in 2013 Euromicro Conference on Digital System Design, 2013, pp. 615–622, doi: 10.1109/DSD.2013.73.
- [29] E. Avaroğlu, T. Tuncer, A. B. Özer, B. Ergen, and M. Türk, "A novel chaos-based post-processing for TRNG," *Nonlinear Dynamics*, vol. 81, no. 1–2, pp. 189–199, 2015.
- [30] T. Tuncer, E. Avaroğlu, M. Türk, and A. B. Ozer, "Implementation of Non-periodic Sampling True Random Number Generator on FPGA," *Informacije MIDEM*, vol. 44, no. 4, pp. 296–302, 2015.
- [31] M. Alçın, İ. Koyuncu, M. Tuna, M. Varan, and İ. Pehlivan, "A novel high speed Artificial Neural Network-based chaotic True Random Number Generator on Field Programmable Gate Array," *International Journal of Circuit Theory and Applications*, vol. 47, no. 3, pp. 365–378, 2019.
- [32] M. Tuna, A. Karthikeyan, K. Rajagopal, M. Alçın, and İ. Koyuncu, "Hyperjerk multiscroll oscillators with megastability: Analysis, FPGA implementation and A Novel ANN-Ring-based True Random Number Generator," *AEU-International Journal of Electronics and Communications*, vol. 112, no. 2019, pp. 152941–10, 2019.
- [33] T. Kaya, "A true random number generator based on a Chua and RO-PUF: design, implementation and statistical analysis," *Analog Integrated Circuits and Signal Processing*, vol. 102, pp. 415–426, 2020.
- [34] A. M. Garipcan and E. Erdem, "Implementation and Performance Analysis of True Random Number Generator on FPGA Environment by Using Non-periodic Chaotic Signals Obtained from Chaotic Maps," *Arabian Journal for Science and Engineering*, vol. 44, no. 11, pp. 9427–9441, 2019.
- [35] T. Tuncer, "The implementation of chaos-based PUF designs in field programmable gate array," *Nonlinear Dynamics*, vol. 86, no. 2, pp. 975–986, 2016.
- [36] P. Prakash, K. Rajagopal, İ. Koyuncu, J.P. Singh, M. Alçın, B.K. Roy, M. Tuna, "A Novel Simple 4-D Hyperchaotic System with a Saddle-Point Index-2 Equilibrium Point and Multistability: Design and FPGA-Based Applications," *Circuits, Systems, and Signal Processing*, vol. 39, pp. 4259–4280, 2020.
- [37] İ. Koyuncu, M. Tuna, İ. Pehlivan, C. B. Fidan, and M. Alçın, "Design, FPGA implementation and statistical analysis of chaos-ring based dual entropy core true random number generator," *Analog Integrated Circuits and Signal Processing*, vol. 102, no. 2, pp. 445–456, 2020.

- [38] S. Jafari, J. C. Sprott and F. Nazarimehr, "Recent new examples of hidden attractors," *The European Physical Journal Special Topics*, vol. 224, no. 8, pp. 1469-1476, 2015.
- [39] M. S. Azzaz, C. Tanougast, S. Sadoudi, R. Fellah, and A. Dandache, "A new auto-switched chaotic system and its FPGA implementation," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 7, pp. 1792-1804, 2013.
- [40] M. Tuna, M. Alçın, İ. Koyuncu, C. B. Fidan, and İ. Pehlivan, "High speed FPGA-based chaotic oscillator design," *Microprocessors and Microsystems*, vol. 66, no. 2019, pp. 72-80, 2019.
- [41] L. Merah, A. Pascha, A. Said and N. H. Mamat, "Design and FPGA implementation of Lorenz chaotic system for information security issues," *Application Mathematics Sciences*, vol. 7, pp. 237-246, 2013.
- [42] İ. Koyuncu, A. T. Özcerit, and İ. Pehlivan, "An analog circuit design and FPGA-based implementation of the Burke-Shaw chaotic system," *Optoelectronics and Advanced Materials-Rapid Communications*, vol. 7, pp. 635-638, 2013.
- [43] İ. Koyuncu, and H. İ. Şeker, "Implementation of Dormand-Prince based chaotic oscillator designs in different IQ-Math number standards on FPGA", *Sakarya Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, vol. 23, no. 5, pp. 859-868, 2019.
- [44] H. İ. Şeker, İ. Koyuncu, M. Tuna and M. Alçın, "Dormand-Prince Tabanlı SEA Kaotik Osilatör Tasarımının FPGA Üzerinde Gerçeklenmesi," *5th International Academic Research Congress*, Ankara, pp. 1-8, 2019.
- [45] Y. Meng, G. Li, D. Yang, and L. Zhan, "A new directional stability transformation method of chaos control for first order reliability analysis," *Structural and Multidisciplinary Optimization*, vol. 55, no. 2, pp. 601-612, 2017.
- [46] Y. Jiang, H. Zhu, and Z. Li, "A new compound faults detection method for rolling bearings based on empirical wavelet transform and chaotic oscillator," *Chaos, Solitons & Fractals*, vol. 89, pp. 8-19, 2016.
- [47] Z. Tian, "Chaotic characteristic analysis of network traffic time series at different time scales," *Chaos, Solitons & Fractals*, vol. 130, pp. 109412, 2020.
- [48] X. Chen, J. Hu, Z. Peng, and C. Yuan, "Bifurcation and chaos analysis of torsional vibration in a PMSM-based driven system considering electromechanically coupled effect" *Nonlinear Dynamics*, vol. 88, no. 1, pp. 277-292, 2017.
- [49] D. Ding, Y. Weng, and N. Wang, "Dynamics analysis of a fractional-order delayed SBT memristive chaotic system without equilibrium points," *The European Physical Journal Plus*, vol. 134, no 444, pp. 1-7, 2019.
- [50] S. Jafari, A. Ahmadi, A. J. M. Khalaf, H. R. Abdolmohammadi, V. T. Pham and F. E. Alsaadi, "A new hidden chaotic attractor with extreme multi-stability," *AEU-International Journal of Electronics and Communications*, vol. 89, pp. 131-135, 2018.

BIOGRAPHIES



İSMAIL KOYUNCU has an MSc from Abant İzzet Baysal University, Bolu-Turkey. He completed his doctoral research in the Department of Electrical and Electronics Engineering at Sakarya University, Sakarya-Turkey in 2014. Since 2017, he is an Associate Professor in the Department of Electrical and Electronics

Engineering at Afyon Kocatepe University, in Afyon-Turkey. His main research interests are FPGA-based digital system design, chaos, TRNG and reconfigurable computing. He is also interested in FPGA-based artificial neural networks and computer graphics.



HALİL İBRAHİM ŞEKER was born in 1994, in Karaman, Turkey. He received the B.S. from Bozok University in 2017, and M.S. degrees, Electrical and Electronics Engineering from Afyon Kocatepe University in 2019, Afyon-Turkey. He is currently conducting his doctoral research in the Department of Electrical and Electronics Engineering at Sakarya University of Applied Sciences, Sakarya-Turkey. His research interests include chaos, FPGA-based digital system design and control theory.



MURAT ALÇIN received the BSc, MSc and PhD degrees in Electronic-Computer Teaching from the University of Marmara, Turkey, in 2006 and in 2009, and department of Electrical and Electronics Engineering at Sakarya University, in Sakarya-Turkey, 2017, respectively. From 2008 to 2012, he was an instructor in Abant İzzet Baysal University Electronic Technology Program at Bolu Vocational School, Bolu-Turkey. Since 2018, he is an Assistant Professor in the Department of Mechatronics Engineering at Afyon Kocatepe University, in Afyon-Turkey. His research interests include Neural Networks, Chaotic Systems and FPGA-based digital system design.



MURAT TUNA received his BSc and MSc in Electrical Education from Kocaeli University of Technical Education, in 2004, and Kocaeli University of Institute of Science, Kocaeli, Turkey, in 2008. He received his PhD in the Department of Electrical and Electronics Engineering at Karabuk University, Karabuk-Turkey in 2017. Currently, he is working at Kırklareli University in Turkey, Assistant Professor, since 2009. His main research topics include chaos, TRNG, FPGA-based digital system design and reconfigurable computing. He is also interested in mathematical model and control of nonlinear systems.