INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2017, VOL. 63, NO. 2, PP. 195–199
Manuscript received February 12, 2017; revised April, 2017. DOI: 10.1515/eletel-2017-0026

Yet Another Pseudorandom Number Generator

Borislav Stoyanov, Krzysztof Szczypiorski, and Krasimir Kordov

***Abstract*—We propose a novel pseudorandom number generator based on Rössler attractor and bent Boolean function. We estimated the output bits properties by number of statistical tests. The results of the cryptanalysis show that the new pseudorandom number generation scheme provides a high level of data security.**

***Keywords*—Rössler attractor, bent Boolean function, pseudorandom number generator**

I. Introduction

BOOLEAN and chaotic functions have been used extensively in the area of a pseudorandom number generations. Novel encryption scheme based on bent Boolean function and feedback with carry shift register is proposed in [32]. In [27], a cryptographic algorithm based on the Lorenz chaotic attractor and 32 bit bent Boolean function is presented.

In [8], a new chaotic system with good cryptographic properties, is proposed. Novel pseudorandom generation algorithm based on Chebyshev polynomial and Tinkerbell map, is provided in [28]. Pseudorandom bit generators, based on the Chebyshev map and rotation equation, are proposed in [29], [33], and [34]. The presented schemes exhibit high level of security. The proposed scheme shows that the output stream possesses suitable properties for security-demanding applications. A modified pseudorandom bit generator, based on Tinkerbell map, is presented in [16]. Pseudorandom zero-one generation algorithm based on two chaotic Circle maps and XOR function is designed in [13]. In [14], pseudorandom number generation scheme, based on Signature attractor is presented.

Pseudorandom bit generation algorithms, based on Circle map and based on Chirikov map are proposed in [30] and in [31].

Several scientific papers present cryptographic primitives build from Rössler attractor.

An algorithm for secure data transmission with Rössler function protection of the information signal is presented in [6]. In [10], an improvement to an existing algorithm used in security data sending by modifying the structure of the Rössler map behaviour, is designed.

A fingerprint image encryption method based on hyperchaotic Rössler map is provided in [1]. The statistical analysis is presented to prove the secrecy of the biometric trait by using novel scheme.

This work is partially supported by the Scientific research fund of Konstantin Preslavski University of Shumen under the grant No. RD-08-121/06.02.2017.

Borislav Stoyanov and Krasimir Kordov are with the Department of Computer Informatics, Konstantin Preslavsky University of Shumen, Bulgaria (e-mails: borislav.stoyanov@shu.bg, krasimir.kordov@shu.bg).

Krzysztof Szczypiorski is with Warsaw University of Technology, Warsaw, Poland; Cryptomage SA, Wroclaw, Poland (e-mail: ksz@tele.pw.edu.pl).

A communication scheme to encrypted audio and image information transmission, based on hyperchaotic generalized Hénon and Rössler maps is designed in [2]. The scheme is suitable in master-slave configuration. Another communication scheme with high stability in the recovered signal, based on Rössler circuit, is presented in [11].

The stability of impulsive synchronization of chaotic and Rössler hyperchaotic systems by using Lyapunov exponent of the variational synchronization error systems are studied in [12].

An algorithm to image encryption by using a Rössler chaotic function is presented in [18]. The approach consists of two substitution methods and two scrambling methods; to change the value of the pixels and the location of the pixels, respectively.

A chaotic permutation for physical layer security in OFDM-PON is presented in [15]. An encryption algorithm based on improved hyperchaotic Rössler map is proposed in [20]. The proposed scheme is attractive for applications in private communication systems.

In [25], design and simulation of synchronization between two identical coupled Röossler circuits, are proposed.

In [4], based on the Rössler attractor, random sequences generator is proposed. The algorithm is SIMULINK modelled and is tested using statistical tests. Random number generator from Rössler attractor also is presented in [5]. The output chaotic signal proposes a negligible value of an autocorrelation function.

A pseudorandom number generator is proposed in this paper. The novel algorithm is based on chaotic function and bent Boolean function. The novelty of our approach lies in the combination of the Rössler attractor and Maiorana function.

In Section 2, we propose novel pseudorandom number generator and its security analysis. Finally, the last section concludes the article.

II. Pseudo-random bit generator from Rössler attractor

A. Rössler chaotic attractor

The famous Rösler attractor is presented in [23], Eq. (1):

$$\begin{aligned} \frac{dx}{dt} &= -y - z \\ \frac{dy}{dt} &= x + ay \\ \frac{dz}{dt} &= b + z(x - c) \ , \end{aligned} \tag{1}$$

where the parameters a, b, and c are positive real numbers. The system is chaotic when $a = 0.2$, $b = 0.2$, and $c = 5.7$. Three-Dimensional model of Rössler Attractor is illustrated in Fig. 1. Fig. 2 shows 2-Dimensional plot of Rössler Attractor. Sensitivity to initial conditions are shown in Fig. 3.

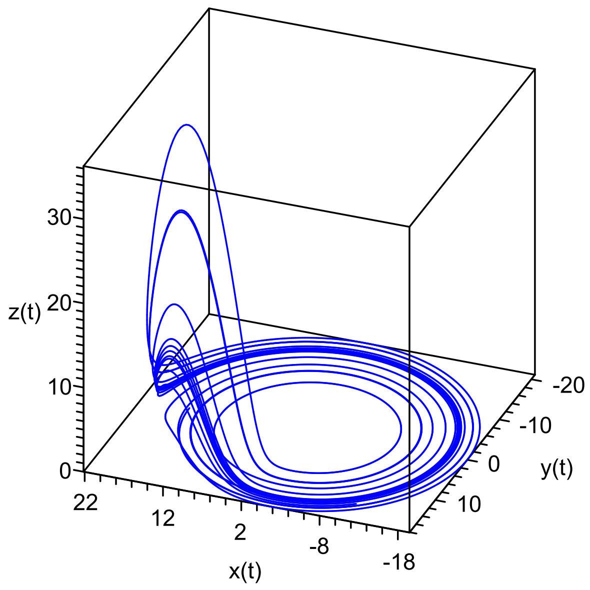


Fig. 1. 3-Dimensional plot of Rössler Attractor

B. Bent Boolean Functions

In this subsection we refer to works of Cusick and Stănică [7], Neumann [19], Pommerening [21], and Rothaus [22].

Definition 1: A Boolean function f in n variables is map from $\mathbb{V}_n$ (the vector space on n dimension) to the two-element Galois field $\mathbb{F}_2$. The (0,1)-sequence defined by $(f(\mathbf{x}_0), f(\mathbf{x}_1), \ldots, f(\mathbf{x}_{2^{n-1}}))$ is called the truth table of f, where $\mathbf{v}_0 = (0, \ldots, 0, 0), \mathbf{v}_1 = (0, \ldots, 0, 1), \ldots, \mathbf{v}_{2^{n-1}} = (1, \ldots, 1, 1)$, ordered by lexicographical order.

To each Boolean function $f : \mathbb{V}_n \to \mathbb{F}_n$ we associate *sign* function, denoted by $\hat{f} : \mathbb{V}_n \to \mathbb{R}^* \subseteq \mathbb{C}^*$ and defined by $\hat{f}(\mathbf{x}) = (-1)^{f(\mathbf{x})}$.

Definition 2: The Walsh transform of a function f on $\mathbb{V}_n$ (with the values of f taken to be real numbers 0 and 1) is the map $W(f) : \mathbb{V}_n \to \mathbb{R}$, defined by

$$W(f)(\mathbf{w}) = \sum_{\mathbf{x} \in \mathbb{V}_n} f(\mathbf{x})(-1)^{\mathbf{w} \cdot \mathbf{x}}$$

which defines the coefficients of f with respect to the orthonormal basis of the group characters $Q_{\mathbf{x}}(\mathbf{w}) = (-1)^{\mathbf{w} \cdot \mathbf{x}}$ (where $\mathbf{w} \cdot \mathbf{x}$ is the scalar product); f can be recovered by the inverse Walsh transform

$$f(\mathbf{x}) = 2^{-n} \sum_{\mathbf{w} \in \mathbb{V}_n} W(f)(\mathbf{w})(-1)^{\mathbf{w} \cdot \mathbf{x}}$$

Definition 3: A Boolean function f in n variables is called *bent* if and only if the Walsh transform coefficients of $\hat{f}$ are all $\pm 2^{n/2}$, that is, $W(\hat{f})^2$ is constant.

Maiorana construction provides us with the following bent function

$$x_0 y_0 \oplus \ldots \oplus x_{m-1} y_{m-1} \oplus x_0 x_1 \cdots x_{m-1}, \tag{2}$$

where the Boolean function is presents by the polynomial $P(x_0, \ldots, x_{m-1}, y_0, \ldots, y_{m-1}) = R(x_0, \ldots, x_{m-1}) \oplus x_0 y_0 \oplus \ldots \oplus x_{m-1} y_{m-1}$ and its dual polynomial $P^\star(x_0, \ldots, x_{m-1}, y_0, \ldots, y_{m-1}) = R(x_0, \ldots, x_{m-1}) \oplus x_0 y_0 \oplus \ldots \oplus x_{m-1} y_{m-1}$, where $R = \mathbb{R}(m)$ is an arbitrary polynomials in m variables.

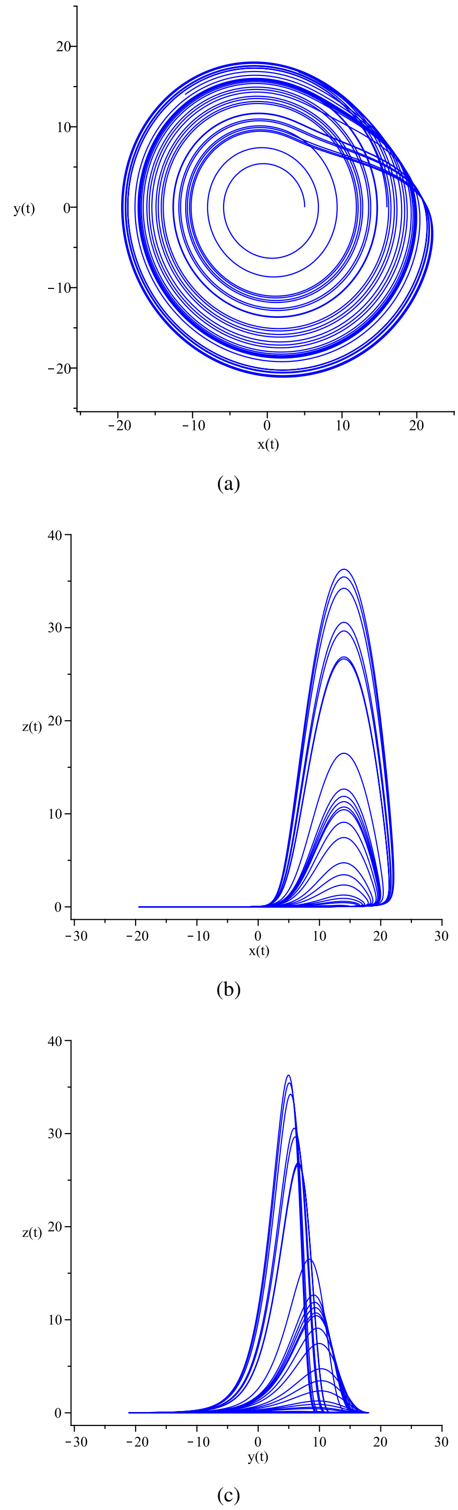


Fig. 2. 2-Dimensional plot of Rössler Attractor: (a) x-y plane, (b) x-z plane, and (c) y-z plane

C. Proposed Bit Generator

The novel algorithm is based on the following steps:

Step 1: The initial values x_0, y_0, and z_0 from Eq. (1) are determined.

Step 2: With using the third-order Runge-Kutta method [9], we numerically compute the attractor from Eq. (1) with step size $h = 0.01$. It is iterated for L_1 times.

Step 3: The iteration of the Eq. (1) continues, and as a result, two real fractions x_i and y_i, are generated and post-processed as follows:

$$s_0 = abs(integer(x_i \times 10^7))$$
$$s_1 = abs(integer(y_i \times 10^7)),$$

where $integer(x)$ returns the integer part of x, truncating the value at the decimal point and $abs(x)$ returns the absolute value of x.

Step 4: Generate a numeric vector $V = (s_0[0], ..., s_0[p], s_1[0], ..., s_1[p])$ that contains the digits of the numbers s_0 and s_1.

Step 5: Apply the vector V to Maiorana function from Eq. (2) to get a single output bit.

Step 6: Return to Step 3 until the bit stream limit is reached.

The proposed bit generator is implemented in C++, using the following initial values: $x_0 = 0.1$, $y_0 = 0.15$, $z_0 = 0.01$, and $L_1 = 2000$.

D. Key space evaluation

The secret key space is composed by the four secret keys x_0, y_0, z_0, and L_1. With number of about 15 decimal digits precision in IEEE double precision [36] the proposed key space is more than 2^{126}, which is good enough against exhaustive key search [3].

E. Statistical tests

Three software test programs are used in order to measure the behaviour of the output binary streams.

The DIEHARD package [17] includes 19 statistical tests: Birthday spacings, Overlapping 5-permutations, Binary rank (31 x 31), Binary rank (32 x 32), Binary rank (6 x 8), Bitstream, Overlapping-Pairs-Sparse-Occupancy, Overlapping-Quadruples-Sparse-Occupancy, DNA, Stream count-the-ones, Byte-count-the-ones, Parking lot, Minimum distance, 3D spheres, Squeeze, Overlapping sums, Runs (up and down), and Craps. The tests return $P - values$, which should be uniform in [0,1), if the input file contains pseudorandom numbers. The $P-values$ are obtained by $p = F(y)$, where F is the assumed distribution of the sample random variable y, often the normal distribution.

The NIST software application [24] is a set of 15 statistical tests: Frequency (monobit), Block-frequency, Cumulative sums (forward and reverse), Runs, Longest run of ones, Rank, Fast Fourier Transform (spectral), Non-overlapping templates, Overlapping templates, Maurers ”Universal Statistical”, Approximate entropy, Random excursion, Random-excursion variant, Serial, and Linear complexity.

The testing process consists of the following steps:

Step 1: State the null hypothesis. Assume that the zero/one sequence is random.

Step 2: Compute a sequence test statistic. Testing is carried out at the bit level.

Step 3: Compute the $P - value$, $P - value \in [0, 1]$.

Step 4: Fix α, where $\alpha \in [0.0001, 0.01]$. Compare the $P - value$ to α. $Success$ is declared whenever $P - value \geq \alpha$; otherwise, $failure$ is declared.

The NIST package calculates the proportion of sequences that pass the particular tests. The range of acceptable proportion is determined using the confidence interval defined as,

$$\hat{p} \pm 3\sqrt{\frac{\hat{p}(1-\hat{p})}{m}},$$

where $\hat{p} = 1 - \alpha$, and m is the number of binary tested sequences. NIST recommends that, for these tests, the user should have at least 1000 sequences of 1000000 bits each. In our setup $m = 1000$. Thus the confidence interval is

$$0.99 \pm 3\sqrt{\frac{0.99(0.01)}{1000}} = 0.99 \pm 0.0094392.$$

The proportion should lie above 0.9805607 with exception of Random excursion and Random excursion variant tests. These two tests only apply whenever the number of cycles in a sequence exceeds 500. Thus the sample size and minimum pass rate are dynamically reduced taking into account the tested sequences.

The distribution of $P - values$ is examined to ensure uniformity. The interval between 0 and 1 is divided into 10 subintervals. The $P - values$ that lie within each subinterval are counted. Uniformity may also be specified through an application of a χ^2 test and the determination of a $P - value$ corresponding to the goodness-of-fit distributional test on the $P - values$ obtained for an arbitrary statistical test, $P - value$ of the $P - values$. This is implemented by calculating

$$\chi^2 = \sum_{i=1}^{10} \frac{(F_i - s/10)^2}{s/10},$$

where F_i is the number of $P - values$ in subinterval i and s is the sample size. A $P - value$ is computed such that $P - value_T = IGAMC(9/2, \chi^2/2)$, where $IGAMC$ is the complemented incomplete gamma statistical function. If $P - value_T \geq 0.0001$, then the sequences can be considered to be uniformly distributed.

The ENT package [35] performs 6 tests to sequences. They are Entropy, Optimum compression, χ^2 distribution, Arithmetic Mean value, Monte Carlo Value for π, and Serial Correlation Coefficient. The sequences of bytes are stored in files. The suite outputs the results of those tests. We tested output stream of 125000000 bytes of the novel pseudorandom number generator.

The test results are given in Table I, Table II, and Table III, respectively. All of statistical tests are passed successfully.

III. Conclusions and Future Work

A novel pseudorandom number generator based on a chaotic map is proposed in this article. The proposed algorithm combines Rössler attractor and Maiorana bent Boolean function.

TABLE I
DIEHARD STATISTICAL TEST RESULTS FOR TWO 80 MILLION BITS SEQUENCES GENERATED BY THE PROPOSED GENERATOR

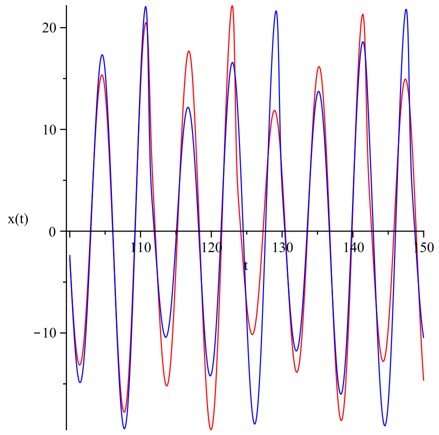
DIEHARD statistical test	**Proposed Generator *P-value***
Birthday spacings	0.593701
Overlapping 5-permutation	0.395409
Binary rank (31 x 31)	0.746323
Binary rank (32 x 32)	0.955445
Binary rank (6 x 8)	0.470244
Bitstream	0.479493
OPSO	0.522760
OQSO	0.569775
DNA	0.509277
Stream count-the-ones	0.213018
Byte count-the-ones	0.612866
Parking lot	0.428480
Minimum distance	0.479449
3D spheres	0.470514
Squeeze	0.935011
Overlapping sums	0.616515
Runs up	0.317489
Runs down	0.347915
Craps	0.587091

TABLE II
NIST STATISTICAL TEST SUITE RESULTS FOR 1000 SEQUENCES OF SIZE 10^6-BIT EACH GENERATED BY THE PROPOSED GENERATOR

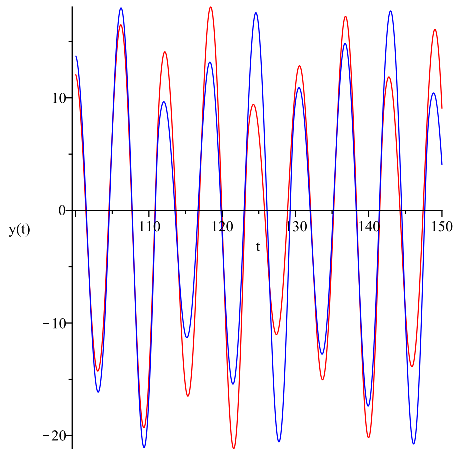
NIST statistical test	**Proposed Generator**	
	P-value	**Pass rate**
Frequency (monobit)	0.896345	991/1000
Block-frequency	0.348869	988/1000
Cumulative sums (Forward)	0.095426	992/1000
Cumulative sums (Reverse)	0.632955	993/1000
Runs	0.195864	992/1000
Longest run of Ones	0.597620	990/1000
Rank	0.587274	992/1000
FFT	0.849708	987/1000
Non-overlapping templates	0.505628	990/1000
Overlapping templates	0.308561	986/1000
Universal	0.474986	988/1000
Approximate entropy	0.973718	987/1000
Random-excursions	0.476145	629/635
Random-excursions Variant	0.502142	630/635
Serial 1	0.707513	997/1000
Serial 2	0.729870	987/1000
Linear complexity	0.096578	993/1000

TABLE III
ENT STATISTICAL TEST RESULTS FOR TWO 80 MILLION BITS SEQUENCES GENERATED BY THE PROPOSED GENERATOR.

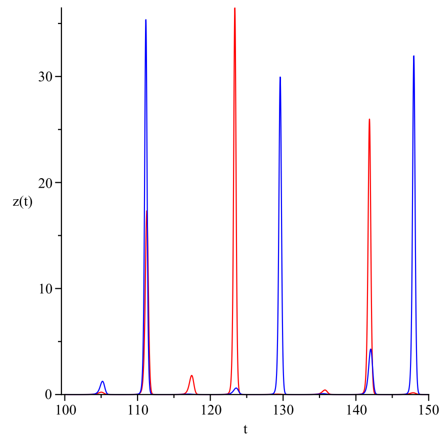
ENT statistical test	**Proposed Generator results**
Entropy	7.999998 bits per byte
Optimum compression	OC would reduce the size of this 125000000 byte file by 0 %.
χ^2 distribution	For 125000000 samples is 271.65, and randomly would exceed this value 22.62 % of the time.
Arithmetic mean value	127.4991 (127.5 = random)
Monte Carlo π estim.	3.141880562 (error 0.01 %)
Serial correl. coeff.	-0.000089 (totally uncorrelated = 0.0)



(a)



(b)



(c)

Fig. 3. Time series plot of Rössler Attractor: (a) t-x plane, (b) t-y plane, and (c) t-z plane. Shows sensitivity to initial conditions with $x_0 = 1$ (blue) and $x_0 = 1.001$ (red).

An accurate security analysis on the novel scheme is given. Based on the results, we can conclude that the proposed pseudorandom number generation algorithm is acceptable for the secure data encryption.

We intend to use this algorithm for Galois field based encryption [26].

ACKNOWLEDGMENT

The authors are grateful to the anonymous referees for valuable and helpful comments.

The authors would like to thank Borislav Bedzhev and Stanimir Stanev for their comments and suggestion on earlier drafts of this paper.

REFERENCES

[1] F. Abundiz-Pérez, C. Cruz-Hernández, M.A. Murillo-Escobar, R.M. López-Gutiérrez, and A. Arellano-Delgado, A Fingerprint Image Encryption Scheme Based on Hyperchaotic Rössler Map, *Mathematical Problems in Engineering*, **2016**, Article ID 2670494, pages 15, 2016.

[2] A.Y. Aguilar-Bustos, C. Cruz-Hernández, R.M. López-Gutiérrez, and C. Posadas–Castillo, Synchronization of Different Hyperchaotic Maps for Encryption, *Nonlinear Dynamics and Systems Theory*, **8**(3), 221–236, 2008.

[3] G. Alvarez, S. Li, Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems, *International Journal of Bifurcation and Chaos,* **16**, 2129–2151, 2006.

[4] C. Banerjee, D. Datta, and D. Datta, A Random Bit Generator Using Rössler Chaotic System, K. Maharatna et al. (eds.), Computational Advancement in Communication Circuits and Systems, *Lecture Notes in Electrical Engineering*, **335**, 81–87, 2015.

[5] V. Canals, A. Morro, and J.L. Rosselló, Random Number Generation Based on the Rossler Attractor, *IEICE Proceeding Series*, **1**, 272–275, 2014.

[6] D. Chantov, A Chaos Based Two-level Secure Communication System on the Basis of two Different Pairs of Synchronized Chaotic Systems, *International Journal on Information Technologies & Security*, **1**, 51–62, 2012.

[7] T. W. Cusick, and P. Stănică, *Cryptographic Boolean Functions and Applications*, Academic Press, 2009.

[8] Dăscălescu, Ana-Cristina and Boriga, Radu Eugen and Diaconu, Adrian-Viorel, Study of a new chaotic dynamical system and its usage in a novel pseudorandom bit generator, *Mathematical Problems in Engineering* **2013**, Article ID 769108, 10 pages, 2013, http://dx.doi.org/10.1155/2013/769108.

[9] I. Faragó, *Numerical Methods for Ordinary Differential Equations*, TypoTech, Budapest, 2014.

[10] M. Frunzete, A.-A. Popescu, and J.-P. Barbot, Dynamical Discrete-Time Rössler Map with Variable Delay, *Lecture Notes in Computer Science*, **9155**, 431–446, 2015.

[11] J.H. García-López, and Jaimes-Reátegui, R. and Pisarchik, A.N. and Murguía-Hernandez, A. and Medina-Gutiérrez, C. and Valdivia-Hernadez, R. and Villafana-Rauda, E., Novel Communication Scheme based on Chaotic Rössler Circuits, *Journal of Physics: Conference Series* **23**(1), 276–284, 2005.

[12] M. Itoh, T. Yang, and L.O. Chua, Conditions for impulsive synchronization of chaotic and hyperchaotic systems, *International Journal of Bifurcation and Chaos*, **11**(2), 551–560, 2001.

[13] K. Kordov, Modified Pseudo-Random Bit Generation Scheme Based on Two Circle Maps and XOR Function, *Applied Mathematical Sciences*, **9**(3), 129–135, 2015.

[14] K. Kordov, Signature Attractor Based Pseudorandom Generation Algorithm, *Advanced Studies in Theoretical Physics*, **9**(6), 287–293, 2015.

[15] B. Liu, and Zhang, Lijia and Xin, Xiangjun and Wang, Yongjun, Physical layer security in OFDM-PON based on dimension-transformed chaotic permutation, *IEEE Photonics Technology Letters*, **26**(2), 127–130, 2014.

[16] D. Malchev, I. Ibryam, Construction of pseudorandom binary sequences using chaotic maps (2015) *Applied Mathematical Sciences*, **9** (77-80), 3847–3853. http://dx.doi.org/10.12988/ams.2015.52149.

[17] G. Marsaglia, *DIEHARD: a Battery of Tests of Randomness*, http://www.fsu.edu/pub/diehard/.

[18] H.M. Al-Najjar, Digital image encryption algorithm based on multi-dimensional chaotic system and pixels location, *International Journal of Computer Theory and Engineering*, **4**(3), 354–357, 2012.

[19] T. Neumann, *Bent Functions*, Doctoral dissertation, University of Kaiserslautern, 2006.

[20] Orozco, Eduardo Rodriguez and Guerrero, E Efren Garcia and González, Everardo Inzunza and Bonilla, Oscar R López, Image Encryption Based on Improved Rössler Hyperchaotic Map, *Difu100ci@ Revista en Ingeniería y Tecnología, UAZ*, **8**(2), 2014.

[21] K. Pommerening, Fourier Analysis of Boolean Maps–A Tutorial, 2005.

[22] O. S. Rothaus, On "bent" functions, *Journal of Combinatorial Theory*, Series A, Volume 20, Issue 3, 1976, 300–305.

[23] O.E. Rössler, An Equation for Continuous Chaos, *Physics Letters*, **57A**(5), 397–398, 1976.

[24] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Application, *NIST Special Publication 800-22*, Revision 1a (Revised: April 2010), Lawrence E. Bassham III, 2010, http://csrc.nist.gov/rng/.

[25] A. Sambas, W.S. Mada Sanjaya, M. Mamat, and Halimatussadiyah, Design and analysis bidirectional chaotic synchronization of Rössler circuit and its application for secure communication, *Applied Mathematical Sciences*, **7**(1), 11–21, 2013.

[26] Zh. Savova-Tasheva, A. Tasheva, Algorithms for Extended Galois Field Generation and Calculation, *Mathematical and Software Engineering*, **1**(1), 18–24, 2015, http://varepsilon.com/index.php/mse/article/view/7.

[27] B.P. Stoyanov, Chaotic cryptographic scheme and its randomness evaluation, in 4th AMiTaNS'12, *AIP Conference Proceedings,* **1487**, 397–404, 2012, http://dx.doi.org/10.1063/1.4758983.

[28] B. Stoyanov, Pseudo-random Bit Generation Algorithm Based on Chebyshev Polynomial and Tinkerbell Map, Applied Mathematical Sciences, Vol. 8, 2014, no. 125, 6205–6210, http://dx.doi.org/10.12988/ams.2014.48676.

[29] B.P. Stoyanov, Pseudo-random bit generator based on Chebyshev map, in 5th AMiTaNS'13, *AIP Conference Proceedings,* **1561** (2013), 369–372, http://dx.doi.org/10.1063/1.4827248.

[30] B.P. Stoyanov, Using Circle Map in Pseudorandom Bit Generation, in 6th AMiTaNS'14, *AIP Conference Proceedings,* **1629** (2014), 460 - 463, http://dx.doi.org/10.1063/1.4902309.

[31] B. Stoyanov, K. Kordov, K., A Novel Pseudorandom Bit Generator Based on Chirikov Standard Map Filtered with Shrinking Rule, *Mathematical Problems in Engineering,* **2014**, Article ID 986174, 2014, 1–4., http://dx.doi.org/10.1155/2014/986174.

[32] B.P. Stoyanov, K.M. Kordov, Cryptanalysis of a modified encryption scheme based on bent Boolean function and Feedback with Carry Shift Register, in 5th AMiTaNS'13, *AIP Conference Proceedings,* **1561**, 373–377, 2013, http://dx.doi.org/10.1063/1.4827249.

[33] B. Stoyanov, K. Kordov, Image encryption using Chebyshev map and rotation equation, Entropy, **17**, 2117–2139, 2015, http://dx.doi.org/10.3390/e17042117.

[34] B. Stoyanov, K. Kordov, Novel Image Encryption Scheme Based on Chebyshev Polynomial and Duffing Map, *The Scientific World Journal* **2014**, Article ID 283639, 1–11, 2014, http://dx.doi.org/10.1155/2014/283639.

[35] J. Walker, *ENT: A Pseudorandom Number Sequence Test Program*, 2008, http://www.fourmilab.ch/random/.

[36] IEEE Computer Society, *754-2008 - IEEE Standard for Floating-Point Arithmetic*, Revision of ANSI/IEEE Std 754-1985, 2008, DOI: 10.1109/IEEESTD.2008.4610935.